

ARITHMETIC OF ABELIAN VARIETIES WITH CONSTRAINED TORSION

CHRISTOPHER RASMUSSEN AND AKIO TAMAGAWA

ABSTRACT. Let K be a number field. We present several new finiteness results for isomorphism classes of abelian varieties over K whose ℓ -power torsion fields are arithmetically constrained for some rational prime ℓ . Such arithmetic constraints are related to an unresolved question of Ihara regarding the kernel of the canonical outer Galois representation on the pro- ℓ fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$.

Under GRH, we demonstrate the set of classes is finite for any fixed K and any fixed dimension. Without GRH, we prove a semistable version of the result. In addition, several unconditional results are obtained when the degree of K/\mathbb{Q} and the dimension of abelian varieties are not too large, through a careful analysis of the special fiber of such abelian varieties. In some cases, the results (viewed as a bound on the possible values of ℓ) are uniform in the degree of the extension K/\mathbb{Q} .

1. INTRODUCTION

1.1. Introduction. Let ℓ be a rational prime number, let μ_N denote the N th roots of unity, and $\mu_{\ell^\infty} = \cup_{n \geq 1} \mu_{\ell^n}$. Set $\mathbb{P}_{01\infty}^1 := \mathbb{P}_{\mathbb{Q}}^1 - \{0, 1, \infty\}$. For a given number field K , we let $\mathbb{T} = \mathbb{T}(K, \ell)$ denote the maximal pro- ℓ extension of $K(\mu_{\ell^\infty})$ which is unramified away from ℓ . Let G_K denote the absolute Galois group $\text{Gal}(\bar{K}/K)$, and consider the natural outer Galois representation $\Phi: G_K \rightarrow \text{Out}(\pi_1^\ell(\mathbb{P}_{01\infty}^1))$. We let $\mathbb{S} = \mathbb{S}(K, \ell)$ denote the subfield of \bar{K} which is fixed by the kernel of Φ . Anderson and Ihara [AI88] have shown that \mathbb{S} is precisely the minimal field of definition (containing K) of all curves appearing in the pro- ℓ tower of (Galois) coverings of \mathbb{P}^1 , branched only over $\{0, 1, \infty\}$. Moreover, they demonstrate many properties of \mathbb{S} , including the containment $\mathbb{S} \subseteq \mathbb{T}$.

Ihara has asked the following question ([Iha86]), which is still open: For $K = \mathbb{Q}$, does $\mathbb{S} = \mathbb{T}$? (The choice of the notation is motivated as follows: the kanji 天, read *ten*, means “heaven,” and the kanji 山, read *san*, means “mountain.” Both 山 and 天 are infinite pro- ℓ extensions of $K(\mu_\ell)$. Ihara’s question is roughly as follows: “Does the mountain reach the heavens?”)

There is a natural source for subextensions of \mathbb{T} . Let A denote an abelian variety over K which possesses good reduction away from ℓ . Then by the theory of Serre-Tate, the extension $K(A[\ell^\infty])/K(A[\ell])$ is pro- ℓ and unramified away from ℓ ; hence, in certain cases one finds $K(A[\ell^\infty]) \subseteq \mathbb{T}$. Reflecting on Ihara’s question, it is natural to then study whether or not $K(A[\ell^\infty]) \subseteq \mathbb{S}$. In several cases where A is the Jacobian variety of a curve C , this is known to occur. For example, the containment holds for the following curves C which appear in the pro- ℓ tower over $\mathbb{P}_{01\infty}^1$:

- Fermat curves and Heisenberg curves for any ℓ [AI88],

- Principal modular curves $X(2^n)$, $\ell = 2$ [AI88],
- Elliptic curves E/\mathbb{Q} , $\ell = 2$ [Ras04],
- Elliptic curves E/\mathbb{Q} , $\ell = 3$ [PR07],
- Modular curves $X(3^n), X_0(3^n), X_1(3^n)$, $\ell = 3$ [PR07].

In addition, those elliptic curves E/\mathbb{Q} with good reduction away from ℓ and which have CM by $\mathbb{Q}(\sqrt{-\ell})$ are also known to satisfy $K(E[\ell^\infty]) \subseteq \text{山}$ [RT08], although they do not lie in the pro- ℓ tower over $\mathbb{P}_{01\infty}^1$.

Despite the existence of these examples, the abelian varieties A/K which satisfy $K(A[\ell^\infty]) \subseteq \text{天}$ appear to be quite rare. For an abelian variety A/K , let $[A]$ denote its K -isomorphism class. For any fixed number field K , fixed integer $g > 0$, and fixed rational prime number ℓ , set

$$(1.1) \quad \mathcal{A}(K, g, \ell) := \{[A] : \dim A = g \text{ and } K(A[\ell^\infty]) \subseteq \text{天}\}.$$

For fixed ℓ , this set is necessarily finite by the Shafarevich Conjecture (Faltings' theorem). We also define

$$(1.2) \quad \mathcal{A}(K, g) := \{([A], \ell) : [A] \in \mathcal{A}(K, g, \ell)\}.$$

Conjecture 1. *For any K and g , the set $\mathcal{A}(K, g)$ is finite. Equivalently, the set $\mathcal{A}(K, g, \ell)$ is non-empty for only finitely many ℓ .*

Remark. If A has everywhere good reduction, it is at least possible that $[A] \in \mathcal{A}(K, g, \ell)$ for more than one ℓ . Hence, the reader should not assume that the natural surjection $\mathcal{A}(K, g) \rightarrow \bigcup_\ell \mathcal{A}(K, g, \ell)$, $([A], \ell) \mapsto [A]$, is a bijection.

In [RT08], the authors prove this conjecture in the case $(K, 1)$ for $K = \mathbb{Q}$ and for K a quadratic extension of \mathbb{Q} other than the nine imaginary quadratic extensions of class number one. Moreover, the set $\mathcal{A}(\mathbb{Q}, 1)$ is determined explicitly. It contains 50 \mathbb{Q} -isomorphism classes, spanning 21 \mathbb{Q} -isogeny classes. The containment related to Ihara's question, $\mathbb{Q}(E[\ell^\infty]) \subseteq \text{山}(\mathbb{Q}, \ell)$ is demonstrated for almost all classes $([E], \ell) \in \mathcal{A}(\mathbb{Q}, 1)$. There are 4 isomorphism classes, spanning 2 isogeny classes, which remain open. In each of these classes, $\ell = 11$ and the representative curve E does *not* have complex multiplication.

In the present article, we prove the finiteness of $\mathcal{A}(K, g)$, for arbitrary K and g , under the assumption of the Generalized Riemann Hypothesis. In addition, several new cases of the conjecture are proven unconditionally. When possible, we give proofs for uniform versions of the conjecture, meaning we demonstrate the existence of a constant C , possibly dependent on g and $[K : \mathbb{Q}]$, but not K itself, so that $\ell > C$ implies $\mathcal{A}(K, g, \ell) = \emptyset$.

The organization of the paper is as follows. In §2, several well-known results from analytic number theory are collected. In §3, the behavior of the Galois representation ρ on $A[\ell]$ is studied for any $[A] \in \mathcal{A}(K, g, \ell)$, leading to constraints on the indices of semistable reduction. This yields a proof of the conjecture when we restrict to abelian varieties with semistable reduction. In §4, we construct a character $\chi(m_{\mathbb{Q}})$ from ρ , and demonstrate the remarkable property that $\chi(m_{\mathbb{Q}})$ never vanishes on the Frobenius elements of small primes. This will play a key role in the proofs of both the conditional and unconditional finiteness results.

In §5, we prove the conjecture under the assumption of the Generalized Riemann Hypothesis in various forms. Actually, two proofs are given. The first proves the finiteness of $\mathcal{A}(K, g)$ for any choice of (K, g) . The second proves a version of the conjecture which is uniform in the degree of K/\mathbb{Q} . Unfortunately, the second

proof requires the assumption that $[K : \mathbb{Q}]$ is odd. Finally, this uniform result is generalized to the case of extensions of odd, bounded degree of a fixed but arbitrary number field F .

The remainder of the paper is dedicated to unconditional proofs of the conjecture for certain choices of K and g . In §6, the behavior of the special fiber is used to further constrain the numerical invariants introduced in §3, §4. These results are then used in §7 to prove the conjecture unconditionally in several new cases:

- $K = \mathbb{Q}$ and $g = 2, 3$,
- $[K : \mathbb{Q}] = 2$ and $g = 1$,
- $[K : \mathbb{Q}] = 3$ and $g = 1$,
- K/\mathbb{Q} is a Galois extension of exponent 3 and $g = 1$.

Moreover, in the case of cubic extensions and $g = 1$, we are able to give a uniform version of the result.

1.2. Notations. For any number field F , we let Δ_F denote the absolute discriminant of F/\mathbb{Q} , and let $n_F = [F : \mathbb{Q}]$. For any extension of number fields E/F , if \mathfrak{P} is a prime of E above a prime \mathfrak{p} of F , we let $e_{\mathfrak{P}/\mathfrak{p}}$ and $f_{\mathfrak{P}/\mathfrak{p}}$ denote, respectively, the ramification index and the degree of the residue field extension. We let $\kappa(\mathfrak{p})$ denote the residue field of \mathfrak{p} .

Throughout, the notation $C_j = C_j(x, y, \dots, z)$ indicates a constant C_j which is dependent on x, y, \dots, z and no other quantities.

2. INGREDIENTS FROM ANALYTIC NUMBER THEORY

In this section, we accumulate a few results from analytic number theory that will be needed in the sequel.

2.1. Prime m -th power residues. Let ℓ be a prime number. Whenever $m \geq 1$ is a divisor of $\ell - 1$, it will be useful to find a small rational prime p which is an m -th power residue modulo ℓ ; that is, for which $p \pmod{\ell} \in \mathbb{F}_\ell^{\times m}$. Without further restriction on m , the best known bound for p is $p = O(\ell^{5.5})$, given by Heath-Brown in [HB92]. However, for $m < 23$, the following result of Elliott gives a stronger bound [Ell71]:

Proposition 2.1. *Let m be a positive integer and $\varepsilon > 0$. There exists a constant $C'_1 = C'_1(m, \varepsilon)$ such that for any prime ℓ , there exists a prime $p < C'_1 \cdot \ell^{\frac{m-1}{4} + \varepsilon}$ which is an m -th power residue modulo ℓ .*

Remark. In fact, Elliott assumes $m \mid \ell - 1$. But note that in case $m \nmid (\ell - 1)$, we have $\mathbb{F}_\ell^{\times m} = \mathbb{F}_{\ell'}^{\times m'}$, where $m' := \gcd(m, \ell - 1) < m$. So in fact the result holds as stated.

We re-interpret Elliott's result as follows. For any integer $g > 0$ and any positive $\varepsilon < \frac{1}{4}$, set

$$C_1 = C_1(m, g, \varepsilon) := (4gC'_1)^{\frac{4}{(5-m)-4\varepsilon}}.$$

Corollary 2.2. *Suppose $1 \leq m \leq 4$ and $0 < \varepsilon < \frac{1}{4}$. For any prime $\ell > C_1$, there exists a prime number $p < \frac{\ell}{4g}$ which is an m -th power residue modulo ℓ .*

Proof. The quantity $\ell^{\frac{m-1}{4} + \varepsilon}$ is sub-linear in ℓ ; hence, there must be some lower bound for which such a p is guaranteed to exist. More precisely, one may check directly that $\ell > C_1$ implies $C'_1 \ell^{\frac{m-1}{4} + \varepsilon} < \frac{\ell}{4g}$. \square

2.2. Goldfeld's Theorem. We recall a result of Goldfeld which will be used in the proof of finiteness over quadratic fields when $g = 1$. Let K be a number field, and let S be a finite set of rational primes. Consider the following two properties possibly satisfied by an integer N :

- (**Go 1**) There is a quadratic extension L/\mathbb{Q} such that $-N$ is the discriminant of L/\mathbb{Q} . (Automatically, $L = \mathbb{Q}(\sqrt{-N})$.)
- (**Go 2**) If $p < \frac{|N|}{4}$ is a rational prime, $p \notin S$, and p splits completely in K , then p does not split in $\mathbb{Q}(\sqrt{-N})$.

The following result of Goldfeld is proved in the Appendix of [Maz78]. (It is unfortunately not effective.)

Theorem 2.3 (Theorem A, [Maz78]). *Consider the set*

$$\mathcal{N}(K, S) := \{N \in \mathbb{Z} : N \text{ satisfies both } (\textbf{Go 1}) \text{ and } (\textbf{Go 2})\}.$$

If $n_K \leq 2$, then $\mathcal{N}(K, S)$ is finite.

We will rely on the following corollary to demonstrate finiteness of $\mathcal{A}(K, 1)$ for quadratic fields K .

Corollary 2.4. *Suppose $n_K = 2$. There exists an ineffective constant $C_2 = C_2(K)$ such that, for any prime $\ell > C_2$, there exists a prime number $p < \frac{\ell}{4g}$ which is a square residue modulo ℓ and which satisfies $f_{\mathfrak{p}/p} = 1$ for any prime \mathfrak{p} of K above p .*

Proof. For any odd prime ℓ , let $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$, and notice that ℓ^* is the discriminant of $\mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}$. Further, p splits in $\mathbb{Q}(\sqrt{\ell^*})$ if and only if $(\frac{p}{\ell}) = 1$. Let us set

$$\mathcal{N}'(K) := \left\{ -\ell^* : \begin{array}{l} \ell \text{ odd prime such that for every } p < \frac{\ell}{4}, \\ \text{if } p \text{ splits in } K \text{ then } (\frac{p}{\ell}) = -1 \end{array} \right\}.$$

As $\mathcal{N}'(K) \subseteq \mathcal{N}(K, \emptyset)$, the result follows immediately. \square

2.3. Chebotarev Density Theorem. Let E/F be a Galois extension of number fields, and let \mathfrak{p} be a prime of F , unramified in E/F . The Frobenius elements of primes \mathfrak{P} of E above \mathfrak{p} form a conjugacy class

$$\left[\frac{E/F}{\mathfrak{p}} \right] := \{\text{Frob}_{\mathfrak{P}} : \mathfrak{P} \subseteq \mathcal{O}_E, \mathfrak{P} \mid \mathfrak{p}\}$$

inside $\text{Gal}(E/F)$. If the particular choice of \mathfrak{P} is irrelevant, and no confusion arises, we will write $\text{Frob}_{\mathfrak{p}}$ to denote any one element from this class.

Let $\sigma \in \text{Gal}(E/F)$. The Chebotarev Density Theorem states that there are infinitely many primes \mathfrak{p} of F , unramified in E/F , for which $\sigma \in \left[\frac{E/F}{\mathfrak{p}} \right]$. We now recall an effective version of this result, due to Lagarias and Odlyzko [LO77], conditional on the Generalized Riemann Hypothesis (GRH).

Theorem 2.5. *There exists an absolute constant $C_3 > 0$ with the following property. Let E/F be a Galois extension of number fields, and suppose the Generalized Riemann Hypothesis holds for the Dedekind zeta function of E . For any $\sigma \in \text{Gal}(E/F)$, there exists a prime \mathfrak{p} of F , unramified in E/F , with the following properties:*

- $\sigma \in \left[\frac{E/F}{\mathfrak{p}} \right]$,
- $N_{F/\mathbb{Q}}\mathfrak{p} \leq C_3(\log \Delta_E)^2$ (provided $E \neq \mathbb{Q}$).

Remark. This statement combines both Corollary 1.2 and the discussion on pages 461–462 of [LO77].

In exchange for a weakening of the bound on the norm, we may place an additional constraint on \mathfrak{p} .

Corollary 2.6. *Let E/F be a Galois extension of number fields, and let \tilde{E} denote the Galois closure of E over \mathbb{Q} . Let σ be a fixed element of $\text{Gal}(E/F)$. Assume GRH holds for the Dedekind zeta function of \tilde{E} . Then there exists a prime \mathfrak{p} of F , unramified in E/F , such that*

- $\sigma \in \left[\frac{E/F}{\mathfrak{p}} \right]$,
- $N_{F/\mathbb{Q}}\mathfrak{p} \leq C_3(\log \Delta_{\tilde{E}})^2$ (provided $E \neq \mathbb{Q}$),
- $f_{\mathfrak{p}/p} = 1$, where p is the rational prime below \mathfrak{p} .

Proof. As σ fixes \mathbb{Q} and $\sigma(E) \subseteq \tilde{E}$, there exists $\tilde{\sigma} \in \text{Gal}(\tilde{E}/\mathbb{Q})$ such that $\tilde{\sigma}|_E = \sigma$. Applying Theorem 2.5 to the extension \tilde{E}/\mathbb{Q} , we know there exists a rational prime $p < C_3(\log \Delta_{\tilde{E}})^2$ such that p is unramified in \tilde{E}/\mathbb{Q} and $\tilde{\sigma} \in \left[\frac{\tilde{E}/\mathbb{Q}}{p} \right]$. Thus, there is a prime ideal $\mathfrak{P} \mid p$ of \tilde{E} such that $\tilde{\sigma} = \text{Frob}_{\mathfrak{P}}$. Necessarily, the decomposition group $D_{\mathfrak{P}} \leq \text{Gal}(\tilde{E}/\mathbb{Q})$ is generated by $\tilde{\sigma}$. As $\tilde{\sigma}$ fixes F , we in fact have $D_{\mathfrak{P}} \leq \text{Gal}(\tilde{E}/F)$. Let F_1 denote the subextension of \tilde{E}/F fixed by $D_{\mathfrak{P}}$, and set $\mathfrak{p}_1 := \mathfrak{P} \cap \mathcal{O}_{F_1}$. Necessarily, the residue fields $\mathcal{O}_{F_1}/\mathfrak{p}_1$ and $\mathbb{Z}/p\mathbb{Z}$ coincide, and so $f_{\mathfrak{p}_1/p} = 1$. Setting $\mathfrak{p} = \mathfrak{p}_1 \cap \mathcal{O}_F$, we have $f_{\mathfrak{p}/p} = 1$, also. Moreover, $\sigma \in \left[\frac{E/F}{\mathfrak{p}} \right]$; since $N_{F/\mathbb{Q}}\mathfrak{p} = p$, the result is shown. \square

Suppose ℓ is a rational prime and $m \mid (\ell - 1)$. We let $\mathbb{Q}(\mu_\ell)_m$ denote the unique subfield of $\mathbb{Q}(\mu_\ell)$ which is a degree m extension of \mathbb{Q} .

Proposition 2.7. *Let $m \geq 1$, $g > 0$, and $n \geq 1$ be fixed integers. Let K be a fixed number field, with Galois closure \tilde{K} over \mathbb{Q} . There exists a constant $C_6 = C_6(m, g, n, K)$ with the following property. Suppose $\ell > C_6$ is a prime number, set $L_0 = \mathbb{Q}(\mu_\ell)_m$, and suppose the Generalized Riemann Hypothesis holds for the Dedekind zeta function of $L_0\tilde{K}$. Then for any $\sigma \in \text{Gal}(L_0\tilde{K}/K)$, there exists a rational prime $p < \left(\frac{\ell}{4g} \right)^{1/n}$ and a prime $\mathfrak{p} \mid p$ of K , such that*

- \mathfrak{p} is unramified in $L_0\tilde{K}/K$,
- $f_{\mathfrak{p}/p} = 1$,
- $\sigma \in \left[\frac{L_0\tilde{K}/K}{\mathfrak{p}} \right]$.

Consequently, for $\ell > C_6$, there exists a prime $p < \left(\frac{\ell}{4g} \right)^{1/n}$ which is an m -th power residue modulo ℓ .

Proof. Since C_6 may depend on K , we may assume $\ell \nmid \Delta_K$ without loss of generality. Let $L = L_0K$, $\tilde{L} = L_0\tilde{K}$. Then \tilde{L} is the Galois closure of L over \mathbb{Q} . The fields L_0 and \tilde{K} are linearly disjoint over \mathbb{Q} and have no common factor in their discriminants. So ([Lan94, Prop. 17]) we have

$$\Delta_{\tilde{L}} = \Delta_{L_0\tilde{K}} = \Delta_{\tilde{K}}^{n_{L_0}} \cdot \Delta_{L_0}^{n_{\tilde{K}}} = \Delta_{\tilde{K}}^m \cdot (\ell^{m-1})^{n_{\tilde{K}}}.$$

Consequently, we always have the bound

$$\begin{aligned} \log \Delta_{\tilde{L}} &= m \log \Delta_{\tilde{K}} + (m-1)n_{\tilde{K}} \log \ell \\ &\leq m \log \Delta_{\tilde{K}} + (m-1)n_K! \log \ell. \end{aligned}$$

If $L = \mathbb{Q}$ (i.e., if $m = 1$ and $K = \mathbb{Q}$), the assertion clearly holds with any $C_6 > 4g \cdot 2^n$, since we may then take $p = 2$. So we may assume $L \neq \mathbb{Q}$. Combining with Corollary 2.6, we see there exists a rational prime p and a prime $\mathfrak{p} \mid p$ of K , such that \mathfrak{p} is unramified in \tilde{L} , $f_{\mathfrak{p}/p} = 1$, and $\sigma \in \left[\frac{\tilde{L}/K}{\mathfrak{p}} \right]$. Moreover, p may be chosen so that

$$(2.1) \quad p \leq C_3 \cdot (C_4 + C_5 \log \ell)^2,$$

where

$$\begin{aligned} C_4 &= C_4(m, K) := m \log \Delta_{\tilde{K}}, \\ C_5 &= C_5(m, n_K) := \max\{1, (m-1)n_K!\}. \end{aligned}$$

As $C_3 \cdot (C_4 + C_5 \log \ell)^2 < \left(\frac{\ell}{4g} \right)^{1/n}$ for $\ell \gg 0$, this proves the first claim. For the second claim, choose $\sigma \in \text{Gal}(\tilde{L}/K)$ such that $\sigma|_{L_0} = \text{id}$. Then the prime \mathfrak{p} guaranteed by the first claim has an associated Frobenius element which is trivial on L_0 ; this implies that p is an m -th power residue modulo ℓ . \square

Remark. Notice that this result generalizes (in fact, implies, under GRH), the earlier results of the section which guarantee a small prime m -th power residue.

Remark. Theorem 2.5 remains valid even if C_3 is replaced by a larger constant. So we may and do assume $C_3 \geq 1$. Let ℓ' denote the largest prime divisor of Δ_K . For the constant C_6 , we may take the value (provided $(m, K) \neq (1, \mathbb{Q})$)

$$C_6(m, g, n, K) := \max \left\{ \ell', 16g^2 C_3^{2n} C_5^{4n} (2n)^{4n} \exp \left(\frac{C_4}{C_5} \right) \right\}.$$

This follows from a lengthy argument that when $\ell > C_6$, ℓ also satisfies the inequality

$$\left(\frac{\ell}{4g} \right)^{1/n} > C_3 \cdot (C_4 + C_5 \log \ell)^2.$$

The details of the argument are given in the appendix.

3. CONSTRAINTS ON THE INDICES OF SEMISTABLE REDUCTION

Let K be a number field, and A/K an abelian variety of dimension $g > 0$. Let ℓ be a rational prime. For any prime λ of K above ℓ , denote by K_λ the λ -adic completion of K . Let A_{K_λ} denote the base change of A over K_λ , and let $e_{A_{K_\lambda}}$ be the minimal ramification index at λ for which semistable reduction for A_{K_λ} is achieved. In this section, we record some constraints on $e_{A_{K_\lambda}}$ in general, and also under the assumption that $[A] \in \mathcal{A}(K, g, \ell)$.

3.1. The index of semistable ramification. Let K_λ^{ur} denote the maximal unramified extension of K_λ , and let $I_\lambda = G_{K_\lambda^{\text{ur}}} \subset G_{K_\lambda}$ denote the inertia group at λ . The ramification index $e_{\lambda/\ell}$ divides $[K_\lambda : \mathbb{Q}_\ell] \leq n_K$. Moreover, $e_{\lambda/\ell} > 1$ for some $\lambda \mid \ell$ if and only if $\ell \mid \Delta_K$. It is known that, for any prime $\ell' \neq \ell$, the kernel J_λ of the natural representation $\rho_{A, \ell'}^{\text{ss}} : I_\lambda \rightarrow \text{GL}(V_{\ell'}(A)^{\text{ss}})$ is an open subgroup of I_λ independent of the choice of ℓ' . Further, J_λ has index $e_{A_{K_\lambda}}$ in I_λ , so we may be

sure that $e_{A_{K_\lambda}} \mid \#\mathrm{GL}_{2g}(\mathbb{F}_{\ell'})$ for every $\ell' \nmid 2\ell$. (These are consequences of [SGA7I, Exposé IX].) Hence, the following is useful:

Lemma 3.1. *Fix an integer $n > 0$. For any prime p and any odd prime ℓ' , the p -part of $\#\mathrm{GL}_n(\mathbb{F}_{\ell'})$ is divisible by p^{u_p} , where*

$$\begin{aligned} u_2 &:= v_2(n!) + n + \lfloor \frac{n}{2} \rfloor, \\ u_p &:= v_p \left(\left\lfloor \frac{n}{p-1} \right\rfloor ! \right) + \left\lfloor \frac{n}{p-1} \right\rfloor \quad (p > 2). \end{aligned}$$

Here, v_p denotes the p -adic valuation, and $\lfloor \cdot \rfloor$ denotes the greatest integer function. Moreover, for any p , there are infinitely many ℓ' such that the p -part of $\#\mathrm{GL}_n(\mathbb{F}_{\ell'})$ is exactly p^{u_p} .

Proof. The result is not new. For the case of odd p , a proof is given in [GL06, Lemma 7]; for the even case, a similar argument can be constructed by considering primes $\ell' \equiv 3 \pmod{8}$. The formulas given in [Ser79, pg. 120] are helpful. \square

Note, in particular, that $u_p = 0$ for $p > n + 1$. Consequently, the product

$$M'(n) := \prod_{p \text{ prime}} p^{u_p}$$

is always finite, and gives the greatest common divisor of $\{\#\mathrm{GL}_n(\mathbb{F}_{\ell'}) : \ell' \nmid 2\ell\}$. The notation $M'(n)$ is inspired by the similarity to the quantity $M(n)$, which gives the least common multiple of all the orders of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$. This was first computed by Minkowski [Min1887] – see [GL06] for a modern account. In any case, we obtain the following:

Corollary 3.2. *The index $e_{A_{K_\lambda}}$ divides $M'(2g)$. Moreover, if p is a prime with $p \mid e_{A_{K_\lambda}}$, then $p \leq 2g + 1$.*

3.2. Structure of G_K -action on ℓ -torsion. For the remainder of this section, we always work under the following assumption:

$$(A1) \quad [A] \in \mathcal{A}(K, g, \ell)$$

Let $\chi: G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}$ denote the cyclotomic character modulo ℓ . Set $\delta := [\mathbb{F}_{\ell}^{\times} : \chi(G_K)]$, and note that δ divides both n_K and $\ell - 1 = \#\mathbb{F}_{\ell}^{\times}$. We let $\rho_{A, \ell}$ denote the representation of G_K -action on $A[\ell]$. If $[A] \in \mathcal{A}(K, g, \ell)$, the abelian variety A must have good reduction away from ℓ . Moreover, the structure of $\rho_{A, \ell}$ is constrained as follows:

Lemma 3.3. *Under (A1), there is a basis of $A[\ell]$ with respect to which*

$$\rho_{A, \ell} = \begin{pmatrix} \chi^{i_1} & * & \cdots & * \\ & \chi^{i_2} & \cdots & * \\ & & \ddots & \vdots \\ & & & \chi^{i_{2g}} \end{pmatrix}.$$

Moreover, the indices i_r may be chosen so that $i_r \in \mathbb{Z} \cap [0, \frac{\ell-1}{\delta})$ for all $1 \leq r \leq 2g$.

Proof. This is an obvious generalization of [RT08, Lemma 3], and in fact, the proof given there may be followed almost verbatim, with $G = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, $N = \mathrm{Gal}(\bar{\mathbb{Q}}/K(\mu_{\ell}))$, $\Delta = \mathrm{Gal}(K(\mu_{\ell})/K)$. In [RT08], it is only claimed that $i_r < \ell - 1$. We may be sure that the stronger bounds on i_r hold, by the following lemma. \square

Lemma 3.4. *Let G be a profinite group, and let $N \triangleleft G$ be a normal pro- ℓ subgroup of G . Suppose that Δ is a finite cyclic group and $\ell \nmid \#\Delta$. Let $\chi: G \rightarrow \Delta$ be a group homomorphism with $\ker \chi = N$, and let $\psi: G \rightarrow \Delta$ be any other group homomorphism. Then there exists $b \in \mathbb{Z} \cap [0, \#\chi(G)]$ such that $\psi = \chi^b$.*

Proof. As $\ell \nmid \#\Delta$, we clearly have $N \leq \ker \psi$. Now, both G/N and $\chi(G)$ are cyclic, so let gN and x be generators of these respective groups such that $\chi(g) = x$. By the containments $N \leq \ker \psi \leq G$, we see $\#\psi(G) = [G : \ker \psi]$ divides $[G : N] = \#\chi(G)$. We must have $\psi(G) \leq \chi(G)$, since these are subgroups of the same cyclic group Δ . So $\psi(g) = x^b$ for some $0 \leq b < \#\chi(G)$. Necessarily, $\psi = \chi^b$. \square

3.3. Tate-Oort Theory. Let L be the Galois extension of K_λ^{ur} of degree $e_{A_{K_\lambda}}$ corresponding to J_λ . Note that the extension L/K_λ^{ur} descends (non-canonically) to a (possibly non-Galois) extension of K_λ of degree $e_{A_{K_\lambda}}$, and even descends to an extension of K of degree $e_{A_{K_\lambda}}$ (by approximation). As A_L is semistable over \mathcal{O}_L , by [SGA7I, Exposé IX, Prop. 5.6], we see that each character $\chi^{i_r}: J_\lambda = G_L \rightarrow \mathbb{F}_\ell^\times$ extends to a finite group scheme over \mathcal{O}_L . Let $\psi_\lambda: J_\lambda \rightarrow \mathbb{F}_\ell^\times$ be the fundamental character over L . Thus, $\chi = \psi_\lambda^{e_\lambda}$ on J_λ , where $e_\lambda := e_{A_{K_\lambda}} \cdot e_{\lambda/\ell}$, by [Ser72, §1, Prop. 8].

By the theory of Tate-Oort [TO70], $\chi^{i_r} = \psi_\lambda^{j_{\lambda,r}}$ on J_λ , where $j_{\lambda,r} \in \mathbb{Z} \cap [0, e_\lambda]$. From this, we obtain:

$$(3.1) \quad e_\lambda i_r \equiv j_{\lambda,r} \pmod{\ell - 1}.$$

Among all primes of K which do not divide ℓ , choose \mathfrak{p}_0 whose residue field $\kappa(\mathfrak{p}_0)$ is of minimal order, and set $q_0 := \#\kappa(\mathfrak{p}_0)$. Considering primes of K above 2 and 3, we see $q_0 \leq 3^{n_K}$ in general and $q_0 \leq 2^{n_K}$ if $\ell \neq 2$. For any integer $n > 0$, let $P_{\mathfrak{p}_0,n} \in \mathbb{Z}[T]$ denote the characteristic polynomial of $\text{Frob}_{\mathfrak{p}_0}^n$ acting on $V_\ell(A)$, which has degree $2g$. Fix an algebraic closure of \mathbb{Q} and let $\{\alpha_{\mathfrak{p}_0,r}\}_{r=1}^{2g}$ denote the roots of $P_{\mathfrak{p}_0,1}$ (counting multiplicity). These roots satisfy $|\alpha_{\mathfrak{p}_0,r}| = q_0^{1/2}$, and the n -th powers of the $\alpha_{\mathfrak{p}_0,r}$ give exactly the roots of $P_{\mathfrak{p}_0,n}$. On the other hand, modulo ℓ , the roots of $P_{\mathfrak{p}_0,n}$ are given by $\{\chi^{i_r}(\text{Frob}_{\mathfrak{p}_0}^n)\}_{r=1}^{2g}$. From this and the congruence (3.1), we have

$$(3.2) \quad \prod_{r=1}^{2g} (T - \alpha_{\mathfrak{p}_0,r}^{e_\lambda}) = P_{\mathfrak{p}_0,e_\lambda}(T) \equiv \prod_{r=1}^{2g} (T - q_0^{j_{\lambda,r}}) \pmod{\ell}.$$

Let

$$S(T, x_1, \dots, x_{2g}) := \prod_{i=1}^{2g} (T - x_i) \in \mathbb{Z}[x_1, \dots, x_{2g}][T],$$

and let $S_k(x_1, \dots, x_{2g})$ denote the coefficient of T^{2g-k} in S . The polynomials S_k are symmetric in the x_j , and so $S_k(\alpha_{\mathfrak{p}_0,1}^n, \dots, \alpha_{\mathfrak{p}_0,2g}^n) \in \mathbb{Z}$ for any $n \geq 1$. Using (3.2), we have

$$(3.3) \quad S_k(\alpha_{\mathfrak{p}_0,1}^{e_\lambda}, \dots, \alpha_{\mathfrak{p}_0,2g}^{e_\lambda}) \equiv S_k(q_0^{j_{\lambda,1}}, \dots, q_0^{j_{\lambda,2g}}) \pmod{\ell}.$$

As S_k is a homogeneous polynomial of degree k with $\binom{2g}{k}$ terms, and $j_{\lambda,r} \leq e_\lambda$, we certainly have by the triangle inequality:

$$\left| S_k(\alpha_{\mathfrak{p}_0,1}^{e_\lambda}, \dots, \alpha_{\mathfrak{p}_0,2g}^{e_\lambda}) - S_k(q_0^{j_{\lambda,1}}, \dots, q_0^{j_{\lambda,2g}}) \right| \leq \binom{2g}{k} \cdot q_0^{e_\lambda k/2} + \binom{2g}{k} q_0^{e_\lambda k}.$$

We add the following assumption:

$$(A2) \quad \ell > \max \left\{ \binom{2g}{k} \left(q_0^{e_\lambda k} + q_0^{\frac{e_\lambda k}{2}} \right) : \lambda \mid \ell, 1 \leq k \leq 2g \right\}.$$

For example, this is certainly satisfied if

$$(3.4) \quad \ell > C_7 = C_7(g, n_K) := 2 \cdot \binom{2g}{g} \cdot 3^{2g \cdot n_K^2 \cdot M'(2g)}.$$

Take $k = 1$; as $q_0 \geq 2$ and $e_\lambda \geq 1$, we note that $\ell > 2g + 1$ always under (A2).

Under (A2), the congruences (3.3) require equality in \mathbb{Z} , which means the sets (possibly with multiplicity) $\{\alpha_{p_0, r}^{e_\lambda}\}_{r=1}^{2g}$ and $\{q_0^{j_{\lambda, r}}\}_{r=1}^{2g}$ must be equal. By the Weil conjectures, we must have $j_{\lambda, r} = \frac{1}{2}e_\lambda$ for each r . Thus, $2 \mid e_\lambda$. Moreover, A_L has good reduction with ℓ -rank 0. (Otherwise, we would have $j_{\lambda, r} = e_\lambda$ for some r .) Combining with (3.1), we obtain:

$$(3.5) \quad e_\lambda i_r \equiv \frac{e_\lambda}{2} \pmod{(\ell - 1)}, \quad 1 \leq r \leq 2g.$$

Set $e = \gcd\{e_\lambda : \lambda \mid \ell\}$.

Lemma 3.5. *Assume (A1) and (A2) hold. Then*

- (a) $e \mid M'(2g)n_K$,
- (b) $e \mid M'(2g)$ if $\ell \nmid \Delta_K$,
- (c) $(e, \ell - 1) = (\frac{e}{2}, \ell - 1)$,
- (d) $4 \mid e$,
- (e) For any $1 \leq r, s \leq 2g$, $\frac{e}{2}(i_r + i_s - 1) \equiv 0 \pmod{(\ell - 1)}$.

Proof. Let n_λ denote the local degree $[K_\lambda : \mathbb{Q}_\ell]$ at λ . As $\sum_{\lambda \mid \ell} n_\lambda = n_K$ and $e_{\lambda/\ell} \mid n_\lambda$, we see that $\gcd\{e_{\lambda/\ell} : \lambda \mid \ell\} \mid n_K$. Now, by Corollary 3.2,

$$e = \gcd\{e_{A_{K_\lambda}} \cdot e_{\lambda/\ell}\} \Big| \gcd\{M'(2g) \cdot e_{\lambda/\ell}\} = M'(2g) \gcd\{e_{\lambda/\ell}\} \Big| M'(2g)n_K,$$

which proves (a). When $\ell \nmid \Delta_K$, all $e_{\lambda/\ell} = 1$, so that $e = \gcd\{e_{A_{K_\lambda}} : \lambda \mid \ell\}$, and (b) follows by Corollary 3.2 also. Since $2 \mid e_\lambda$ for all λ , e must be even. Now, from (3.5), we deduce

$$(3.6) \quad \frac{e}{2}(2i_r - 1) \equiv 0 \pmod{(\ell - 1)}.$$

As $(2i_r - 1)$ is odd, this implies $\text{ord}_2(e) > \text{ord}_2(\ell - 1)$. Thus, (c) holds. Under (A2), $\ell > 2$, so $\text{ord}_2(e) > 1$, proving (d). Finally, adding the congruence (3.6) for two indices $1 \leq r, s \leq 2g$ gives

$$e(i_r + i_s - 1) \equiv 0 \pmod{(\ell - 1)}.$$

This, combined with (c), implies (e). \square

Already, we may prove a finiteness result for everywhere semistable abelian varieties. For fixed K, g, ℓ , let $\mathcal{A}^{\text{ss}}(K, g, \ell)$ denote the subset of $\mathcal{A}(K, g, \ell)$ containing only classes of abelian varieties with everywhere semistable reduction; likewise, let $\mathcal{A}^{\text{ss}}(K, g)$ denote the set of pairs $([A], \ell) \in \mathcal{A}(K, g)$ for which A has everywhere semistable reduction.

Theorem 3.6. *For any K and any $g > 0$, the set $\mathcal{A}^{\text{ss}}(K, g)$ is finite. Equivalently, $\mathcal{A}^{\text{ss}}(K, g, \ell) = \emptyset$ for $\ell \gg 0$.*

Proof. For sufficiently large ℓ , we may be sure that both $\ell \nmid \Delta_K$, and that (A2) holds. Suppose $[A] \in \mathcal{A}^{\text{ss}}(K, g, \ell)$. As $\ell \nmid \Delta_K$, we know $e_{\lambda/\ell} = 1$ for every prime $\lambda \mid \ell$ in K . Hence, $e_\lambda = e_{A_{K_\lambda}}$ for every λ . But as A is already semistable at λ , $e_{A_{K_\lambda}} = 1$. Thus $e_\lambda = 1$, and so $e = 1$ also. But under (A2), $e > 1$, a contradiction. Thus, $\mathcal{A}^{\text{ss}}(K, g, \ell) = \emptyset$. \square

In fact, a uniform version of Theorem 3.6 is available for many values of n_K .

Lemma 3.7. *Suppose $[A] \in \mathcal{A}(K, g, \ell)$ and $\ell > C_7(g, n_K)$.*

- (a) *If $2 \nmid e_{A_{K_\lambda}}$ for every $\lambda \mid \ell$, then $4 \mid n_K$.*
- (b) *If $4 \nmid e_{A_{K_\lambda}}$ for every $\lambda \mid \ell$, then $2 \mid n_K$.*

Proof. By Lemma 3.5, we know $4 \mid e_{A_{K_\lambda}} e_{\lambda/\ell}$ for each $\lambda \mid \ell$. If $2 \nmid e_{A_{K_\lambda}}$ for every λ , then we must have $4 \mid e_{\lambda/\ell}$. Since $n_K = \sum_{\lambda \mid \ell} e_{\lambda/\ell} f_{\lambda/\ell}$, we obtain (a). Part (b) may be argued the same way. \square

Thus, we obtain a uniform version of Theorem 3.6 for many values of n_K .

Corollary 3.8. *Let n be a positive integer, not divisible by 4. For any number field K/\mathbb{Q} with $n_K = n$, any integer $g > 0$, and any rational prime $\ell > C_7(g, n)$, $\mathcal{A}^{\text{ss}}(K, g, \ell) = \emptyset$.*

Proof. Were $\mathcal{A}^{\text{ss}}(K, g, \ell)$ non-empty, it would contain a class $[A]$ for which $e_{A_{K_\lambda}} = 1$ for every $\lambda \mid \ell$. However, this contradicts Lemma 3.7(a). \square

Remark. Note that the proof of Theorem 3.6 actually yields a stronger result, as we only need the existence of one $\lambda \mid \ell$ for which A possesses semistable reduction. Hence, we have actually proven the finiteness of the subset of pairs $([A], \ell)$ in $\mathcal{A}(K, g)$ for which A possesses semistable reduction for at least one prime of K dividing ℓ . (To be clear, this improvement is not available in the uniform version of the corollary, which requires semistable reduction at every prime above ℓ .)

4. SUPERSINGULARITY AT SMALL PRIMES

4.1. The homomorphism ϵ . We keep the notations of the previous section, and assume the hypotheses (A1) and (A2) hold. Recall χ denotes the cyclotomic character modulo ℓ . For any r and s with $1 \leq r, s \leq 2g$, set $\varepsilon_{r,s} := \chi^{i_r + i_s - 1}$. We further define

$$\begin{aligned} \epsilon &:= (\varepsilon_{r,s})_{1 \leq r,s \leq 2g}: G_{\mathbb{Q}} \longrightarrow (\mathbb{F}_\ell^\times)^{(2g)^2}, \\ \epsilon_0 &:= (\varepsilon_{r,r})_{1 \leq r \leq 2g}: G_{\mathbb{Q}} \longrightarrow (\mathbb{F}_\ell^\times)^{2g}. \end{aligned}$$

Set $m_{\mathbb{Q}} := \#\epsilon(G_{\mathbb{Q}})$, and $m_{0,\mathbb{Q}} := \#\epsilon_0(G_{\mathbb{Q}})$. Then $m_{\mathbb{Q}}$ is the least common multiple of the orders of the $\varepsilon_{r,s}$, and $m_{0,\mathbb{Q}}$ is likewise the least common multiple of the orders of the $\varepsilon_{r,r}$. Hence, $m_{0,\mathbb{Q}} \mid m_{\mathbb{Q}}$. Clearly ϵ factors through \mathbb{F}_ℓ^\times , so $m_{\mathbb{Q}} \mid (\ell - 1)$ and $\epsilon(G_{\mathbb{Q}})$ is cyclic. Further, the image has exponent $\frac{\ell}{2}$, by Lemma 3.5(e). Thus, $m_{\mathbb{Q}} \mid \frac{\ell}{2}$, and so $m_{0,\mathbb{Q}} \mid m_{\mathbb{Q}} \mid (\frac{\ell}{2}, \ell - 1)$.

Lemma 4.1. *We have $m_{0,\mathbb{Q}} = m_{\mathbb{Q}}$. Moreover, $\text{ord}_2 m_{\mathbb{Q}} = \text{ord}_2(\ell - 1)$. In particular, $2 \mid m_{\mathbb{Q}}$.*

Proof. For any r and s , note that $\varepsilon_{r,r} \cdot \varepsilon_{s,s} = \varepsilon_{r,s}^2$. Thus, $m_{\mathbb{Q}} \mid 2m_{0,\mathbb{Q}}$. We certainly have:

$$\text{ord}_2(m_{0,\mathbb{Q}}) \leq \text{ord}_2(m_{\mathbb{Q}}) \leq \text{ord}_2\left(\frac{\ell}{2}, \ell - 1\right) \leq \text{ord}_2(\ell - 1).$$

Since $\chi^{(2i_r-1)m_{0,\mathbb{Q}}} = \varepsilon_{r,r}^{m_{0,\mathbb{Q}}} = 1$, we have $(2i_r-1)m_{0,\mathbb{Q}} \equiv 0 \pmod{\ell-1}$. Since $2i_r-1$ is odd, it follows that $\text{ord}_2 m_{0,\mathbb{Q}} \geq \text{ord}_2(\ell-1)$, and so all four terms in the inequality are equal. This implies $m_{\mathbb{Q}} \mid m_{0,\mathbb{Q}}$, and so $m_{\mathbb{Q}} = m_{0,\mathbb{Q}}$. \square

4.2. The characters $\chi(m)$. Let m be an integer dividing $\ell-1$. We let $\chi(m) : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^{\times}/\mathbb{F}_{\ell}^{\times m}$ denote the character χ modulo m -th powers. Then the character $\chi(m_{\mathbb{Q}})$ carries essentially the same information as the homomorphism ϵ . Indeed, we have just seen that ϵ factors through $\mathbb{F}_{\ell}^{\times}$. Since the image is cyclic of order $m_{\mathbb{Q}}$, we have an isomorphism $\mathbb{F}_{\ell}^{\times}/\mathbb{F}_{\ell}^{\times m_{\mathbb{Q}}} \cong \epsilon(G_{\mathbb{Q}})$, and the following diagram commutes:

$$\begin{array}{ccccc} & & \epsilon(G_{\mathbb{Q}}) & & \\ & \swarrow \epsilon & \uparrow & \searrow \cong & \\ G_{\mathbb{Q}} & \xrightarrow{\chi} & \mathbb{F}_{\ell}^{\times} & \xrightarrow{\quad} & \mathbb{F}_{\ell}^{\times}/\mathbb{F}_{\ell}^{\times m_{\mathbb{Q}}} \\ & \searrow & \downarrow & \nearrow & \\ & & \chi(m_{\mathbb{Q}}) & & \end{array}$$

Let $p \neq \ell$ be a rational prime. Since $\chi(\text{Frob}_p) \equiv p \pmod{\ell}$, we see that $\epsilon(\text{Frob}_p)$ is trivial precisely when p is an $m_{\mathbb{Q}}$ -th power residue modulo ℓ .

4.3. A Technique of Mazur. In [Maz78, §7], Mazur deduces congruences from the existence of an isogeny of elliptic curves. Here, we follow the spirit of Mazur's idea and use it to study the behavior of $\chi(m_{\mathbb{Q}})$. Fix a prime number ℓ , a number field K , and $g > 0$. Suppose A/K is an abelian variety for which (A1) and (A2) hold. Let p be a rational prime, and suppose \mathfrak{p} is a prime of K which divides p . We let $q = N_{K/\mathbb{Q}}\mathfrak{p} = p^{f_{\mathfrak{p}}/p}$. Finally, let $\text{Frob}_{\mathfrak{p}} \in G_K$ denote a Frobenius element associated to \mathfrak{p} .

Proposition 4.2. *Suppose $f_{\mathfrak{p}/p}$ is odd, and $q < \frac{\ell}{4g}$. Then $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) \neq 1$.*

Proof. For the sake of contradiction, suppose $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) = 1$; in particular, this forces $\varepsilon_{r,s}(\text{Frob}_{\mathfrak{p}}) = 1$ for all r, s . Let $\{\alpha_{\mathfrak{p},r}\}_{r=1}^{2g}$ be the eigenvalues for $\text{Frob}_{\mathfrak{p}}$. Note that $\{\alpha_{\mathfrak{p},r}^n\}$ are the eigenvalues for $\text{Frob}_{\mathfrak{p}}^n$. If we let $a_{\mathfrak{p},n} (= \sum_{r=1}^{2g} \alpha_{\mathfrak{p},r}^n) \in \mathbb{Z}$ denote the trace of $\text{Frob}_{\mathfrak{p}}^n$, we have:

$$\begin{aligned} a_{\mathfrak{p},2} &= \text{tr}(\text{Frob}_{\mathfrak{p}}^2) \equiv \sum_{r=1}^{2g} \chi^{i_r}(\text{Frob}_{\mathfrak{p}}^2) = \sum_{r=1}^{2g} \chi^{2i_r-1}(\text{Frob}_{\mathfrak{p}}) \cdot \chi(\text{Frob}_{\mathfrak{p}}) \\ &= \sum_{r=1}^{2g} \varepsilon_{r,r}(\text{Frob}_{\mathfrak{p}}) \cdot \chi(\text{Frob}_{\mathfrak{p}}) = 2g\chi(\text{Frob}_{\mathfrak{p}}) \equiv 2gq \pmod{\ell}. \end{aligned}$$

On the other hand, from the Weil conjectures, we know the $\alpha_{\mathfrak{p},r}$ are q -Weil numbers, and so the trace $a_{\mathfrak{p},2}$ is a rational integer satisfying $|a_{\mathfrak{p},2}| \leq 2gq$. As $q < \frac{\ell}{4g}$, we must have $a_{\mathfrak{p},2} = 2gq$. This forces $\alpha_{\mathfrak{p},r}^2 = q$ for all r (any other choice of eigenvalues gives $a_{\mathfrak{p},2} < 2gq$). Consequently:

$$\alpha_{\mathfrak{p},r} = \pm q^{1/2} = \pm p^{f_{\mathfrak{p}/p}/2}.$$

Let s^+ and s^- denote, respectively, the number of indices r for which $\alpha_{\mathfrak{p},r}$ is $+q^{1/2}$ or $-q^{1/2}$. Then the rational integer $a_{\mathfrak{p},1}$ satisfies

$$a_{\mathfrak{p},1} = (s^+ - s^-)p^{f_{\mathfrak{p}/p}/2},$$

which is only possible (since $f_{\mathfrak{p}/p}$ is odd) if $s^+ = s^-$ and $a_{\mathfrak{p},1} = 0$. We now have:

$$\begin{aligned} 0 = a_{\mathfrak{p},1}^2 &= (\text{tr Frob}_{\mathfrak{p}})^2 \equiv \left(\sum_{r=1}^{2g} \chi^{i_r}(\text{Frob}_{\mathfrak{p}}) \right)^2 = \sum_{r=1}^{2g} \sum_{s=1}^{2g} \chi^{i_r+i_s}(\text{Frob}_{\mathfrak{p}}) \\ &= \sum_{r,s} \varepsilon_{r,s}(\text{Frob}_{\mathfrak{p}}) \cdot \chi(\text{Frob}_{\mathfrak{p}}) \equiv 4g^2q \pmod{\ell}. \end{aligned}$$

Consequently, $\ell \mid 4g^2q$, or what is the same, $\ell \mid 4gq$. Clearly this contradicts $q < \frac{\ell}{4g}$, and so it must be that $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) \neq 1$, as claimed. \square

Corollary 4.3. *In case $K = \mathbb{Q}$ we have $\chi(m_{\mathbb{Q}})(\text{Frob}_p) \neq 1$ for all $p < \frac{\ell}{4g}$.*

Moreover, also in the special case $K = \mathbb{Q}$, we have the following result. For any positive $\varepsilon < \frac{1}{12}$, set

$$C_8 = C_8(g, \varepsilon) := \max \left\{ C_7(g, 1), C_1(2, g, \varepsilon), C_1(4, g, \varepsilon), (4gC'_1(2, \varepsilon)^3)^{4/(1-12\varepsilon)} \right\}.$$

Proposition 4.4. *Suppose $0 < \varepsilon < \frac{1}{12}$ and $\ell > C_8$. If $[A] \in \mathcal{A}(\mathbb{Q}, g, \ell)$, then $m_{\mathbb{Q}} > 6$.*

Proof. As $\ell > C_7(g, 1)$, (A2) holds and $m_{\mathbb{Q}}$ must be even. If $m_{\mathbb{Q}} \leq 4$, then by Corollary 2.2, there is a prime $p < \frac{\ell}{4g}$ which is an $m_{\mathbb{Q}}$ -th power residue modulo ℓ . Thus, $\chi(m_{\mathbb{Q}})(\text{Frob}_p) = 1$, which contradicts the previous result. It only remains to eliminate the possibility $m_{\mathbb{Q}} = 6$. We argue by contradiction. Suppose $m_{\mathbb{Q}} = 6$, so that $6 \mid (\ell - 1)$. By Proposition 2.1, we know there exists $p < C'_1(2, \varepsilon) \cdot \ell^{1/4+\varepsilon}$ such that $\chi(2)(\text{Frob}_p) = 1$. As $\ell > (4gC'_1(2, \varepsilon)^3)^{4/(1-12\varepsilon)}$, we have

$$p^3 < C'_1(2, \varepsilon)^3 \cdot \ell^{3/4+3\varepsilon} < \frac{\ell}{4g}.$$

A priori, the characters $\varepsilon_{r,s}$ always take values in μ_6 . However, as p is a square modulo ℓ , we must have $\varepsilon_{r,s}(\text{Frob}_p) \in \mu_3$. Hence

$$\begin{aligned} a_{p,6} &= \text{tr}(\text{Frob}_p^6) \equiv \sum_{r=1}^{2g} \chi^{i_r}(\text{Frob}_p^6) = \sum_{r=1}^{2g} \chi^{2i_r}(\text{Frob}_p^3) \\ &= \sum_{r=1}^{2g} \varepsilon_{r,r}(\text{Frob}_p)^3 \chi(\text{Frob}_p)^3 \equiv 2gp^3 \pmod{\ell}. \end{aligned}$$

From the Weil conjectures, however, we have $|a_{p,6}| \leq 2gp^3$, and so we must have $a_{p,6} = 2gp^3$. Consequently:

$$2gp^3 = \alpha_{p,1}^6 + \cdots + \alpha_{p,2g}^6.$$

As each $\alpha_{p,r}$ has absolute value $p^{1/2}$, we must have $\alpha_{p,r}^6 = p^3$, hence $\alpha_{p,r} = \eta^{t_r} p^{1/2}$, where $0 \leq t_r \leq 5$ and η is a primitive sixth root of unity. Thus, $\alpha_{p,r} \in \mathbb{Q}(\eta, \sqrt{p})$. For each $0 \leq t \leq 5$, set $\kappa_t := \#\{r : \alpha_{p,r} = \eta^t p^{1/2}\}$. The group $\text{Gal}(\mathbb{Q}(\eta, \sqrt{p})/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where

$$\sigma: \begin{cases} \sqrt{p} &\mapsto -\sqrt{p} \\ \eta &\mapsto \eta \end{cases}, \quad \tau: \begin{cases} \sqrt{p} &\mapsto \sqrt{p} \\ \eta &\mapsto \eta^{-1} \end{cases}.$$

As a set (possibly with multiplicity), $\{\alpha_{p,1}, \dots, \alpha_{p,2g}\}$ is Galois stable, which yields $\kappa_0 = \kappa_3$ and $\kappa_1 = \kappa_2 = \kappa_4 = \kappa_5$. Moreover,

$$a_{p,j} = p^{j/2} ((1 + (-1)^j)\kappa_0 + (\eta^j + \eta^{2j} + \eta^{4j} + \eta^{5j})\kappa_1),$$

which vanishes if j is odd. So $a_{p,3} = 0$. Consequently,

$$\begin{aligned} 0 = a_{p,3}^2 &= (\text{tr}(\text{Frob}_p^3))^2 \equiv \left(\sum_{r=1}^{2g} \chi^{i_r}(\text{Frob}_p^3) \right)^2 = \sum_{r=1}^{2g} \sum_{s=1}^{2g} \chi^{i_r}(\text{Frob}_p^3) \chi^{i_s}(\text{Frob}_p^3) \\ &= \sum_{r=1}^{2g} \sum_{s=1}^{2g} \varepsilon_{r,s}(\text{Frob}_p)^3 \chi(\text{Frob}_p)^3 = 4g^2 \chi(\text{Frob}_p)^3 \equiv 4g^2 p^3 \pmod{\ell}. \end{aligned}$$

As ℓ is prime, this implies $\ell \mid 2gp$. However, since $p < p^3 < \frac{\ell}{4g}$, this is impossible; thus, $m_{\mathbb{Q}} \neq 6$. \square

5. CONDITIONAL RESULTS

In this section, we provide two proofs of the finiteness conjecture (Conjecture 1) under the assumption of the Generalized Riemann Hypothesis. The first proof is completely general, in that it demonstrates the finiteness of $\mathcal{A}(K, g)$ for any K/\mathbb{Q} . The second result is weaker, because we must add the assumption that n_K is odd. However, it is a finiteness result which is uniform in the degree n_K ; that is, we demonstrate the existence of one bound L , dependent only on g and n_K , but not K itself, for which $\ell > L$ implies $\mathcal{A}(K, g, \ell) = \emptyset$.

5.1. Finiteness via Effective Chebotarev.

Theorem 5.1. *Let K be a number field, and let $g > 0$. For all $\ell \gg 0$, assume the Generalized Riemann Hypothesis holds for the Dedekind zeta functions of number fields of the form $L\tilde{K}$, where L is a subfield of $\mathbb{Q}(\mu_{\ell})$. Then $\mathcal{A}(K, g)$ is finite.*

Remark. In fact, we need only assume the Generalized Riemann Hypothesis for the Dedekind zeta functions of $L\tilde{K}$, where $L = \mathbb{Q}(\mu_{\ell})_m$ and $m \mid (M'(2g)n_K, \ell - 1)$.

Proof. We show $\mathcal{A}(K, g, \ell)$ is non-empty for only finitely many ℓ . First, let us define:

$$C_9(m, g, K) := \max\{C_6(m, g, 1, K) : m \mid \frac{1}{2}M'(2g)n_K\}$$

Let ℓ be a prime number with

$$\ell > \max\{C_7(g, n_K), C_9(m, g, K)\}.$$

We claim $\mathcal{A}(K, g, \ell) = \emptyset$. If not, then there exists an abelian variety A/K with $[A] \in \mathcal{A}(K, g, \ell)$. Then (A2) holds, and we define the quantities e and $m_{\mathbb{Q}}$ associated to A as in §3, §4, respectively. By Lemma 3.5 and the observation $m_{\mathbb{Q}} \mid \frac{e}{2}$ (§4.1), we have $\ell > C_6(m_{\mathbb{Q}}, g, 1, K)$, so we may apply Proposition 2.7 (with $L_0 = \mathbb{Q}(\mu_{\ell})_{m_{\mathbb{Q}}}$ and $\sigma = 1$). Thus, there exist a rational prime $p < \frac{\ell}{4g}$ and a prime $\mathfrak{p} \mid p$ in K , for which $f_{\mathfrak{p}/p} = 1$, and for which $\left[\frac{L_0\tilde{K}/K}{\mathfrak{p}} \right] = \{1\}$. As $\chi(m_{\mathbb{Q}})|_{G_K}$ factors through $G_K \rightarrow \text{Gal}(L_0\tilde{K}/K)$, it follows that $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) = 1$. On the other hand, by Proposition 4.2, we know $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) \neq 1$, a contradiction. \square

5.2. A Uniform Version. Let F be a field and $n > 0$ an integer. Define the following collection of extensions of F :

$$\mathcal{F}(F, n) := \{K : F \subset K, [K : F] = n\}.$$

Conjecture 2 (Uniform Version). *Let $g > 0$ and $n > 0$. Then there exists a bound $N = N(g, n) > 0$ such that $\mathcal{A}(K, g, \ell) = \emptyset$ for any $K \in \mathcal{F}(\mathbb{Q}, n)$ and any prime $\ell > N$.*

We remark that the uniform version for $n = 1$ is exactly equivalent to the original finiteness conjecture for $\mathcal{A}(\mathbb{Q}, g)$. Thus, when considering the uniform version, we may assume $n > 1$. In this section, we prove the following version of the uniform conjecture:

Theorem 5.2. *Assume the Generalized Riemann Hypothesis. Then Conjecture 2 holds for any g and any odd n .*

In fact, we will prove a stronger result, of which Theorem 5.2 is the specific case $F = \mathbb{Q}$.

Theorem 5.3. *Let F be any number field, and assume the Generalized Riemann Hypothesis for all Dedekind zeta functions of number fields. For any $g > 0$ and any odd $n > 0$, there exists a bound $N = N(g, n, F)$ such that $\mathcal{A}(K, g, \ell) = \emptyset$ for any $K \in \mathcal{F}(F, n)$ and any prime $\ell > N$.*

Remark. The assumption of GRH is only needed for the Dedekind zeta functions of number fields of the form LK , where $L \subseteq \mathbb{Q}(\mu_\ell)$ for some prime ℓ , and K/F is an extension of degree n .

Proof. Set $\mathcal{M}(g, n, F) := \{m \in \mathbb{Z}_{>0} : m \mid \frac{1}{2}M'(2g)n_F n\}$. Define

$$\begin{aligned} N_1 &= N_1(g, n, F) := \max\{C_6(m, g, n, F) : m \in \mathcal{M}(g, n, F)\}, \\ N &= N(g, n, F) := \max\{N_1, C_7(g, n_F n)\}. \end{aligned}$$

Suppose $\ell > N$ is a prime number. Let $K \in \mathcal{F}(F, n)$ (and hence $n_K = n_F n$), and for the sake of contradiction, suppose $[A] \in \mathcal{A}(K, g, \ell)$. By the definition of N , $\ell > C_7(g, n_K)$, and so (A2) holds. By Lemma 3.5 and §4.1, we know the quantities $m_{\mathbb{Q}}$ and e associated to A satisfy $m_{\mathbb{Q}} \mid \frac{e}{2} \mid \frac{1}{2}M'(2g)n_F n$. Now, again by the definition of N , $\ell > C_6(m_{\mathbb{Q}}, g, n, F)$.

Let \tilde{F} denote the Galois closure of F over \mathbb{Q} , and set $\tilde{L} := \mathbb{Q}(\mu_\ell)_{m_{\mathbb{Q}}} \tilde{F}$. We have assumed $\ell > C_6(m_{\mathbb{Q}}, g, n, F)$, and so Proposition 2.7 applies. Thus, there exists a rational prime $p < (\frac{\ell}{4g})^{1/n}$ and a prime \mathfrak{p}_F of F dividing p for which $f_{\mathfrak{p}_F/p} = 1$; moreover, we may assume p is an $m_{\mathbb{Q}}$ -th power modulo ℓ . Thus, $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}_F}) = 1$.

However, as $n = [K : F]$ is odd, we may choose a prime $\mathfrak{p} \mid \mathfrak{p}_F$ of K such that $f_{\mathfrak{p}/\mathfrak{p}_F}$ is odd. Thus $f_{\mathfrak{p}/p} = f_{\mathfrak{p}/\mathfrak{p}_F} \cdot f_{\mathfrak{p}_F/p}$ is odd and at most n , and $N_{K/\mathbb{Q}}\mathfrak{p} = p^{f_{\mathfrak{p}/p}} \leq p^n < \frac{\ell}{4g}$. Hence, by Proposition 4.2, $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) \neq 1$. But $\text{Frob}_{\mathfrak{p}} = \text{Frob}_{\mathfrak{p}_F}^{f_{\mathfrak{p}/\mathfrak{p}_F}}$, so $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}_F}) \neq 1$, which gives a contradiction. \square

Remark. Fix an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} . For a number field $K \subset \bar{\mathbb{Q}}$, $g > 0$, and a prime ℓ , define $\bar{\mathcal{A}}(K, g, \ell)$ to be the image of $\mathcal{A}(K, g, \ell)$ in the set $\mathcal{A}(\bar{\mathbb{Q}}, g)$ of isomorphism classes of g -dimensional abelian varieties over $\bar{\mathbb{Q}}$. For any $n > 0$, define

$$\mathcal{A}(n, g, \ell) := \bigcup_{K \subset \bar{\mathbb{Q}}, K \in \mathcal{F}(\mathbb{Q}, n)} \bar{\mathcal{A}}(K, g, \ell) \subseteq \mathcal{A}(\bar{\mathbb{Q}}, g).$$

Conjecture 2 may be restated as follows: Given $n > 0$ and $g > 0$, $\mathcal{A}(n, g, \ell) = \emptyset$ for ℓ sufficiently large. One might hope that even the set $\mathcal{A}(n, g, \ell)$ is always finite, but this is not the case.

Proposition 5.4. *$\mathcal{A}(2, 1, 2)$ is infinite.*

Proof. For each $i \geq 0$, let $K_i \subseteq \bar{\mathbb{Q}}$ be the splitting field for $x^2 + 2^{i+1}x - 1$, and let ϵ_i denote the root of this polynomial given by $-2^i + \sqrt{2^{2i} + 1}$. Then $[K_i : \mathbb{Q}] = 2$ for all i . Moreover, as the defining polynomial is monic with unit constant term, $\epsilon_i \in \mathcal{O}_{K_i}^\times$. On the other hand, $\epsilon_i - 1$ satisfies $x^2 + (2^{i+1} + 2)x + 2^{i+1}$, and so $\epsilon_i - 1$ lies in $\mathcal{O}_{K_i} \cap \mathcal{O}_{K_i}[\frac{1}{2}]^\times$.

Let E_i be the elliptic curve over K_i defined by the equation $y^2 = x(x-1)(x-\epsilon_i)$. Immediately we see that E_i has good reduction away from 2. Moreover, $E_i[2]$ is rational over K_i , and so $[E_i] \in \mathcal{A}(K_i, 1, 2)$. However, this family corresponds to infinitely many distinct j -invariants, and so the collection $\{[E_i \times_{K_i} \bar{\mathbb{Q}}]\}$ is an infinite subset of $\mathcal{A}(2, 1, 2)$. \square

6. INGREDIENTS FROM THE STRUCTURE OF THE SPECIAL FIBER

6.1. Constraints from the action of inertia, I. The aim of this section is to state and prove a formula relating the dimension of an abelian variety to certain invariants. This will extend the results of [Tam95, §2] into a more general setting. We return to the notations of §3. In particular, the extension L/K_λ^{ur} corresponds to a subgroup J_λ of I_λ . Let $\kappa = \kappa(\lambda)$ denote the residue field of \mathcal{O}_{K_λ} , and let $M := I_\lambda/J_\lambda$.

Let \mathcal{A} be the semistable Néron model of $A_L := A_{K_\lambda} \times_{K_\lambda} L$ over \mathcal{O}_L . Then the Néron property implies that the natural action of M on A_L (which is compatible with the natural faithful action on L) extends to an action of M on \mathcal{A} (itself compatible with the natural faithful action on \mathcal{O}_L). The latter action induces a natural action of M on the special fiber, here denoted $\mathcal{A}_{\bar{\kappa}}$. It also induces a natural action on the connected component $B := \mathcal{A}_{\bar{\kappa}}^0$ at the origin. The actions of M on $\mathcal{A}_{\bar{\kappa}}$ and B are compatible with the natural action of M on $\bar{\kappa}$, which is trivial as M is a quotient of I_λ . Equivalently, M acts on $\mathcal{A}_{\bar{\kappa}}$ and B over $\bar{\kappa}$. As A_L has semistable reduction, B is a semi-abelian variety over $\bar{\kappa}$. Let T denote the torus part of B , so that we have the following canonical exact sequence:

$$(6.1) \quad 0 \longrightarrow T \longrightarrow B \longrightarrow \overline{B} \longrightarrow 0 ,$$

where $\overline{B} := B/T$ is an abelian variety over $\bar{\kappa}$. As this exact sequence is canonical, the action of M preserves it. In particular, M acts on T and \overline{B} .

Let $A_{K_\lambda}^\vee$ be the dual abelian variety of A_{K_λ} over K_λ , and fix a polarization $\pi: A_{K_\lambda} \rightarrow A_{K_\lambda}^\vee$ over K_λ . For each prime $\ell' \neq \ell, \pi$ induces an isomorphism

$$(6.2) \quad V_{\ell'}(A_{K_\lambda}) \rightarrow V_{\ell'}(A_{K_\lambda}^\vee)$$

of G_{K_λ} -modules. In particular, the field L^\vee , defined to be the minimal Galois extension of K_λ^{ur} over which $A_{K_\lambda}^\vee$ obtains semistable reduction, coincides with L . Hence, the analogous quantities for the dual $A_{K_\lambda}^\vee$ also coincide with those for A_{K_λ} . That is, $e_{A_{K_\lambda}^\vee} = e_{A_{K_\lambda}}$, $J_\lambda^\vee = J_\lambda$, etc. If we denote by \mathcal{A}^\vee the semistable Néron model of $A_L^\vee := A_{K_\lambda}^\vee \times_{K_\lambda} L$ over \mathcal{O}_L , we similarly obtain a canonical exact sequence

$$(6.3) \quad 0 \longrightarrow T^\vee \longrightarrow B^\vee \longrightarrow \overline{B}^\vee \longrightarrow 0 ,$$

where B^\vee is the connected component of $\mathcal{A}_{\bar{\kappa}}^\vee$ at the origin, etc.

In the current context, we let $(\cdot)^*$ denote the functor $X \mapsto \text{Hom}(X, \mathbb{Q}_{\ell'}(1))$.

Lemma 6.1. *Let $\ell' \neq \ell$ be a prime number. Then*

$$(6.4) \quad V_{\ell'}(A_{K_\lambda})^{\text{ss}} \cong V_{\ell'}(B) \oplus V_{\ell'}(T^\vee)^*$$

as M -modules.

Proof. Set $V := V_{\ell'}(A_{K_\lambda})$ and $V^\vee := V_{\ell'}(A_{K_\lambda}^\vee)$. As above, we let \mathcal{A}^\vee denote the semistable Néron model of A_L^\vee over \mathcal{O}_L . Then there is a natural perfect pairing

$$(6.5) \quad V \times V^\vee \longrightarrow \mathbb{Q}_{\ell'}(1).$$

Furthermore, by [SGA7I, Exposé IX], V and V^\vee admit the following natural filtrations:

$$(6.6) \quad V \supseteq V^f \supseteq V^t \supseteq \{0\}, \quad V^\vee \supseteq (V^\vee)^f \supseteq (V^\vee)^t \supseteq \{0\}.$$

Here, we have the following definitions/equalities:

$$(6.7) \quad \begin{aligned} V^f &:= V^{J_\lambda} = V_{\ell'}(B), \\ (V^\vee)^f &:= (V^\vee)^{J_\lambda} = V_{\ell'}(B^\vee), \\ V^t &:= V_{\ell'}(T), \\ (V^\vee)^t &:= V_{\ell'}(T^\vee). \end{aligned}$$

With respect to the pairing (6.5), V^t and $(V^\vee)^f$ are exact annihilators of each other. Likewise, V^f and $(V^\vee)^t$ are exact annihilators of each other. Since the action of J_λ on V is unipotent of level ≤ 2 (meaning that for every $\xi \in J_\lambda$, $(\xi - \text{id})^2 = 0$ on V), we have

$$(6.8) \quad V^{\text{ss}} \cong V^{J_\lambda} \oplus (V/V^{J_\lambda}) = V^f \oplus (V/V^f) \cong V^f \oplus ((V^\vee)^t)^*$$

as M -modules, as desired. \square

Let $M' = \langle \gamma \rangle$ be a cyclic subgroup of M , and let e' be the order of M' . We consider the group algebras $\mathbb{Z}[M']$ and $\mathbb{Q}[M']$ of M' over \mathbb{Z} and \mathbb{Q} , respectively. Note that we have:

$$(6.9) \quad \mathbb{Q}[M'] \cong \mathbb{Q}[x]/(x^{e'} - 1) \cong \prod_{d|e'} \mathbb{Q}(\zeta_d),$$

where the isomorphisms are given by identifying the generators $\gamma, x \pmod{x^{e'} - 1}$, and $(\zeta_d)_{d|e'}$ in each algebra. For each divisor $d | e'$, let $\Phi_d(x) \in \mathbb{Z}[x]$ denote the d -th cyclotomic polynomial. Then $\Phi_d(\gamma) \in \mathbb{Z}[M']$ generates \mathfrak{a}_d , the kernel of the natural homomorphism $\mathbb{Z}[M'] \rightarrow \mathbb{Z}[\zeta_d]$ defined by $\gamma \mapsto \zeta_d$.

There is a natural \mathbb{Z} -algebra homomorphism $\mathbb{Z}[M'] \rightarrow \text{End}(B)$, and so we may consider the quotient group scheme $B_d := B/\mathfrak{a}_d B$ of B , on which $\mathbb{Z}[M']$ acts via $\mathbb{Z}[M'] \rightarrow \mathbb{Z}[M']/\mathfrak{a}_d \cong \mathbb{Z}[\zeta_d]$. Similarly, we have homomorphisms from $\mathbb{Z}[M']$ into the endomorphism rings of T , B^\vee and T^\vee , and so we may define quotient group schemes $T_d := T/\mathfrak{a}_d T$, $B_d^\vee := B^\vee/\mathfrak{a}_d B^\vee$, $T_d^\vee := T^\vee/\mathfrak{a}_d T^\vee$. We observe by [Tam95,

Lem. 2.1(i)] that $V_{\ell'}(B_d)$ and $V_{\ell'}(T_d^\vee)$ are free $\mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}$ -modules. Define

$$\begin{aligned} b_d &:= \text{rank}_{\mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}} V_{\ell'}(B_d), \\ t_d &:= \text{rank}_{\mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}} V_{\ell'}(T_d^\vee), \\ n_d &:= b_d + t_d, \\ g_d &:= \dim B_d = \dim B_d^\vee, \\ h_d &:= \dim T_d = \dim T_d^\vee. \end{aligned}$$

Proposition 6.2. *Let φ denote Euler's totient function. There are non-negative integers n_d , indexed by the divisors of e' , such that*

$$(6.10) \quad 2g = \sum_{d|e'} n_d \varphi(d), \quad e' = \text{lcm}\{d : n_d > 0\}.$$

Moreover, if $d \leq 2$, then $2 \mid n_d$.

Proof. The indices n_d will be precisely as defined above. Note that $V_{\ell'}(T_d^\vee)^*$ is also a free $\mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}$ -module of rank t_d . Indeed, this follows from the fact that the automorphism $\gamma \mapsto \gamma^{-1}$ of the group algebra $\mathbb{Z}[M']$ induces an automorphism of $\mathbb{Z}[\zeta_d]$ (namely, $\zeta_d \mapsto \zeta_d^{-1}$). Further, the natural morphisms

$$(6.11) \quad B \rightarrow \bigoplus_{d|e'} B_d, \quad T^\vee \rightarrow \bigoplus_{d|e'} T_d^\vee$$

induce isomorphisms

$$\begin{aligned} (6.12) \quad V^f &= V_{\ell'}(B) \cong \bigoplus_{d|e'} V_{\ell'}(B_d) \\ (V^\vee)^t &= V_{\ell'}(T^\vee) \cong \bigoplus_{d|e'} V_{\ell'}(T_d^\vee), \end{aligned}$$

respectively. The latter decomposition induces $V_{\ell'}(T^\vee)^* \cong \bigoplus_{d|e'} V_{\ell'}(T_d^\vee)^*$. In summary:

$$(6.13) \quad V_{\ell'}(A_{K_\lambda})^{\text{ss}} \cong V_{\ell'}(B) \oplus V_{\ell'}(T^\vee)^* \cong \bigoplus_{d|e'} (V_{\ell'}(B_d) \oplus V_{\ell'}(T_d^\vee)^*).$$

Of course, $\mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}$ has dimension $\varphi(d)$ as a $\mathbb{Q}_{\ell'}$ -vector space, so by counting the dimensions of $\mathbb{Q}_{\ell'}$ -vector spaces on each side of (6.13), we obtain $2g = \sum_{d|e'} n_d \varphi(d)$. As M acts on $V_{\ell'}(A_{K_\lambda})^{\text{ss}}$ faithfully, we must have $\text{lcm}\{d : d \mid e', n_d > 0\} = e'$.

Next, we observe that $h_d = t_d \varphi(d)$, and also

$$\begin{aligned} b_d \varphi(d) &= \dim_{\mathbb{Q}_{\ell'}} V_{\ell'}(B_d) \\ &= \dim_{\mathbb{Q}_{\ell'}} V_{\ell'}(\overline{B}_d) + \dim_{\mathbb{Q}_{\ell'}} V_{\ell'}(T_d) \\ &= 2(g_d - h_d) + h_d = 2g_d - t_d \varphi(d). \end{aligned}$$

Consequently $2g_d = n_d \varphi(d)$. Finally, for $1 \leq d \leq 2$, we have $\varphi(d) = 1$, and so $2 \mid n_d$ as claimed. \square

This allows us to improve the result of Corollary 3.2.

Proposition 6.3. *Let p be a prime divisor of e' . Then*

$$p \leq 2 \cdot \max_{d|e'} \{g_d\} + 1.$$

Proof. By the lcm property satisfied by e' , there exists $d \mid e'$, $n_d > 0$, such that $p \mid d$. Then

$$p = \varphi(p) + 1 \leq \varphi(d) + 1 \leq n_d \varphi(d) + 1 = 2g_d + 1. \quad \square$$

Corollary 6.4. *If $\ell > 2g + 1$, then $e_{A_{K_\lambda}}$ is prime to ℓ , and M is cyclic.*

Proof. If $e_{A_{K_\lambda}} = \#M$ is divisible by ℓ , then there exists a cyclic subgroup M' of M of order $e' = \ell$. By the previous proposition (or Corollary 3.2), we then have $\ell \leq 2g + 1$, which contradicts the assumption. Since $e_{A_{K_\lambda}}$ is prime to ℓ , M arises as a tame inertia group, which is therefore cyclic. \square

Thus, if $\ell > 2g + 1$, we may apply the results in this section to $M' = M$ and $e' = e_{A_{K_\lambda}}$.

6.2. Constraints from the action of inertia, II. Let us continue the notations of the previous subsection. However, we now let d denote a fixed divisor of $e_{A_{K_\lambda}}$, and keep d fixed throughout the current subsection. We will deduce further constraints under the following assumptions:

$$(A3) \quad A_L \text{ has good reduction.}$$

$$(A4) \quad \ell \nmid e_{A_{K_\lambda}}.$$

Remark. If we assume both (A1) and (A2), then (A3) and (A4) hold automatically. For (A3), this follows from the discussion prior to Lemma 3.5. For (A4), this follows from Corollary 3.2 and the observation that $\ell > 2g + 1$ under (A2).

Under (A4), M is cyclic. Under (A3), $B = \mathcal{A}_{\bar{\kappa}}^0 = \mathcal{A}_{\bar{\kappa}}$; we obtain the following decomposition and associated formula

$$B \sim \bigoplus_{d \mid e_{A_{K_\lambda}}} B_d, \quad 2g = \sum_{d \mid e_{A_{K_\lambda}}} n_d \varphi(d).$$

Let γ_d denote the ℓ -rank of B_d , so that $0 \leq \gamma_d \leq g_d$. (As we typically will assume (A1) and (A2), usually $\gamma_d = 0$. See the discussion prior to Lemma 3.5.) Let f and f_λ denote, respectively, the orders of $\ell \pmod{d}$ and $\ell^{f_\lambda/\ell} \pmod{d}$ in $(\mathbb{Z}/d\mathbb{Z})^\times$.

Let us consider the decomposition of A_L in more detail. The uniqueness of L , together with the fact that $K_\lambda^{\text{ur}}/K_\lambda$ is a Galois extension, implies that L/K_λ is Galois. We have the following exact sequence:

$$1 \longrightarrow \text{Gal}(L/K_\lambda^{\text{ur}}) \longrightarrow \text{Gal}(L/K_\lambda) \longrightarrow \text{Gal}(K_\lambda^{\text{ur}}/K_\lambda) \longrightarrow 1.$$

As $\text{Gal}(K_\lambda^{\text{ur}}/K_\lambda) \cong G_{\kappa(\lambda)} \cong \hat{\mathbb{Z}}$ is a free profinite group, this exact sequence splits. So there is a group-theoretic section $s: \text{Gal}(K_\lambda^{\text{ur}}/K_\lambda) \hookrightarrow \text{Gal}(L/K_\lambda)$. Let L_0/K_λ be the subextension of L/K_λ corresponding to the subgroup $\text{Im}(s) \subseteq \text{Gal}(L/K_\lambda)$. Then L_0/K_λ is a finite, totally ramified extension of degree $e_{A_{K_\lambda}}$, and $L = L_0 K_\lambda^{\text{ur}}$.

In case A_L has good reduction, then the inertia group $I_{L_0} \leq G_{L_0}$ acts trivially on $V_{\ell'}(A_{K_\lambda})$ (as before, ℓ' is a prime distinct from ℓ). Hence, $A_{L_0} := A_{K_\lambda} \times_{K_\lambda} L_0$ has good reduction. Let \mathcal{A}_0 be the proper smooth Néron model of A_{L_0} over \mathcal{O}_{L_0} , and let B_0 be the special fiber $(\mathcal{A}_0)_{\kappa(\lambda)}$ of \mathcal{A}_0 . As A_{L_0} has good reduction, B_0 is an abelian variety over $\kappa(\lambda)$. Necessarily, $B = B_0 \times_{\kappa(\lambda)} \overline{\kappa(\lambda)}$.

Note that the abelian subvariety $\mathfrak{a}_d B \subseteq B$ is stable under the action of $G_{\kappa(\lambda)} = \text{Gal}(\overline{\kappa(\lambda)}/\kappa(\lambda))$. This follows from the fact that the prime ideal $\mathfrak{a}_d \subseteq \mathbb{Z}[M]$ is

stable under the natural action of $G_{\kappa(\lambda)}$ (induced by the natural action of $G_{\kappa(\lambda)}$ on M). Thus, the abelian subvariety $\mathfrak{a}_d B \subset B$ and the quotient abelian variety $B \rightarrow B/\mathfrak{a}_d B = B_d$ descend to a unique abelian subvariety and a unique quotient abelian variety $B_0 \rightarrow B_{0,d}$, respectively.

Let $\text{Frob}_\lambda \in G_{\kappa(\lambda)}$ denote the $\ell^{f_\lambda/\ell}$ -th power Frobenius element of $G_{\kappa(\lambda)}$, and let

$$F_\lambda \in \text{End}_{\kappa(\lambda)}(B_{0,d}) \subseteq \text{End}_{\overline{\kappa(\lambda)}}(B_d)_{\mathbb{Q}} = \text{End}(B_d)_{\mathbb{Q}}$$

be the $\ell^{f_\lambda/\ell}$ -th power Frobenius endomorphism. It is well-known that on $V_{\ell'}(B_d)$ the actions of F_λ and Frob_λ coincide with each other. Since $\text{End}(B_d)_{\mathbb{Q}} \subseteq \text{End}(V_{\ell'}(B_d))$, this implies that the conjugate action of F_λ on $\text{End}(B_d)_{\mathbb{Q}}$ induces an action of $\mathbb{Q}(\zeta_d) \hookrightarrow \text{End}(B_d)_{\mathbb{Q}}$ (provided $n_d > 0$, of course). Necessarily, this coincides with the natural (Galois) action of Frob_λ on $\mathbb{Q}(\zeta_d)$. Note that the latter action is induced by $\ell^{f_\lambda/\ell} \pmod{d} \in (\mathbb{Z}/d\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$. In particular, we get that $F := F_\lambda^{f_\lambda}$ acts trivially on $\mathbb{Q}(\zeta_d)$. Equivalently, F and $\mathbb{Q}(\zeta_d)$ commute with each other in $\text{End}(B_d)_{\mathbb{Q}}$. So let $\mathbb{Q}(\zeta_d)'$ denote the centralizer of $\mathbb{Q}(\zeta_d)$ in $\text{End}(B_d)_{\mathbb{Q}}$. We have shown:

Proposition 6.5. *If (A3) and (A4) hold, then $\mathbb{Q}(\zeta_d)[F] \subseteq \mathbb{Q}(\zeta_d)'$.*

Lemma 6.6. *If $n_d = 1$, then $\mathbb{Q}(\zeta_d)' = \mathbb{Q}(\zeta_d)$.*

Proof. Certainly $\mathbb{Q}(\zeta_d)$ commutes with itself, and so we need only demonstrate that $\mathbb{Q}(\zeta_d)' \subseteq \mathbb{Q}(\zeta_d)$. However, $V_{\ell'}(B_d)$ is a free $\mathbb{Q}(\zeta_d) \otimes \mathbb{Q}_{\ell'}$ -module of rank $n_d = 1$. Hence $\mathbb{Q}(\zeta_d)' \otimes \mathbb{Q}_{\ell'} \subseteq \mathbb{Q}(\zeta_d) \otimes \mathbb{Q}_{\ell'}$, which is only possible if $\mathbb{Q}(\zeta_d)' \subseteq \mathbb{Q}(\zeta_d)$. \square

The next proposition demonstrates the implications among the following conditions:

- (C1) $\gamma_d = 0$ and $g_d \leq 2$,
- (C2) $-1 \pmod{d} \in \langle \ell \pmod{d} \rangle$ in $(\mathbb{Z}/d\mathbb{Z})^\times$,
- (C3) B_d is supersingular (i.e., isogenous to a product of supersingular elliptic curves),
- (C4) $\gamma_d = 0$,
- (C5) $\gamma_d < g_d$ or $g_d = 0$,
- (C6) either $2 \mid f$ or $d \leq 2$,
- (C7) $2 \mid n_d f$,
- (C8) $n_d f_\lambda f_{\lambda/\ell} \neq 1$.

Proposition 6.7. (i) *Under assumptions (A3) and (A4), the following implications always hold:*

$$\begin{array}{ccccc} & & (C1) & & \\ & & \Downarrow & & \\ (C2) & (C3) & \Rightarrow & (C4) & \Rightarrow (C5) \\ \Downarrow & \Downarrow & & & \Downarrow \\ (C6) & \Rightarrow (C7) & \xlongequal{\quad} & & (C8) \end{array}$$

(ii) Moreover, if $n_d = 1$, we also have $(C2) \Rightarrow (C3)$ and $(C7) \Rightarrow (C6)$. That is, the following implications hold:

$$\begin{array}{c} (C1) \\ \Downarrow \\ (C2) \Rightarrow (C3) \Rightarrow (C4) \Rightarrow (C5) \\ \Downarrow \quad \Downarrow \quad \Downarrow \\ (C6) \Leftrightarrow (C7) \xrightarrow{\qquad\qquad\qquad} (C8) \end{array}$$

Remark. Before starting the proof, we make the following observations:

- If $(C2)$ does not hold then instead of $(C6)$ we have $2 \mid r := \frac{\varphi(d)}{f}$.
- From the definitions, we have $f_\lambda = \frac{f}{(f, f_{\lambda/\ell})}$. Note that if $f_{\lambda/\ell} = 1$ and $n_d = 1$, then $(C8)$ is equivalent to $d \nmid (\ell - 1)$. (This occurs, for example, when $K = \mathbb{Q}$, $\lambda = (\ell)$, and $n_d = 1$.)

Proof. First, let us show that $(C2)$ implies $(C6)$. Notice that $-1 \equiv 1 \pmod{d}$ is equivalent to $1 \leq d \leq 2$. Otherwise, $-1 \pmod{d} \in (\mathbb{Z}/d\mathbb{Z})^\times$ has order exactly 2, and so $2 \mid f$.

Apart from $(C2)$ and $(C6)$, every condition clearly holds if $n_d = 0$, so we assume $n_d > 0$ for the remainder. The implications $(C1) \Rightarrow (C3) \Rightarrow (C4) \Rightarrow (C5)$ are clear.

Assume $(C6)$. If $2 \mid f$, then of course $(C7)$ holds. If $d \leq 2$, then by Proposition 6.2, $2 \mid n_d$ and again $(C7)$ holds. If $n_d = 1$, we clearly have the reverse implication.

Assume $(C7)$. By the remark above, note that $f_\lambda f_{\lambda/\ell} = \frac{f_{\lambda/\ell}}{(f, f_{\lambda/\ell})} f$, and so is divisible by f . Hence, $2 \mid n_d f_\lambda f_{\lambda/\ell}$, and so $(C8)$ holds.

Now, assume $(C3)$. We may write $B_d \sim E^{g_d}$ for some supersingular elliptic curve E . Then $\text{End}(B_d)_\mathbb{Q} \cong M_{g_d}(D)$, where $D = \text{End}(E)_\mathbb{Q}$ is a quaternion algebra over \mathbb{Q} whose set of ramified primes is exactly $\{\ell, \infty\}$. (This determines D uniquely up to isomorphism.) In particular, $\text{End}(B_d)_\mathbb{Q}$ is a central simple algebra over \mathbb{Q} and we have $\dim_{\mathbb{Q}} \text{End}(B_d)_\mathbb{Q} = \dim_{\mathbb{Q}} M_{g_d}(D) = 4g_d^2$. As $n_d > 0$, we have $\mathbb{Q}(\zeta_d) \hookrightarrow \text{End}(B_d)_\mathbb{Q}$. Let $\mathbb{Q}(\zeta_d)'$ denote the centralizer of $\mathbb{Q}(\zeta_d)$ in $\text{End}(B_d)_\mathbb{Q}$. Then, by [Coh77, Thm. 10.7.5], $\mathbb{Q}(\zeta_d)'$ is a central simple algebra over $\mathbb{Q}(\zeta_d)$,

$$\dim_{\mathbb{Q}(\zeta_d)} \mathbb{Q}(\zeta_d)' = \frac{(2g_d)^2}{\varphi(d)^2} = n_d^2,$$

and

$$\text{End}(B_d)_\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d) \cong M_{\varphi(d)}(\mathbb{Q}(\zeta_d)').$$

However, $\text{End}(B_d)_\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ is also isomorphic to $M_{g_d}(D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d))$, and so $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ and $\mathbb{Q}(\zeta_d)'$ are similar (i.e., the elements of $\text{Br}(\mathbb{Q}(\zeta_d))$ associated to these algebras coincide).

If $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ splits, i.e., $D \cong M_2(\mathbb{Q}(\zeta_d))$, let μ be any prime of $\mathbb{Q}(\zeta_d)$ dividing ℓ . Then $f = [\mathbb{Q}(\zeta_d)_\mu : \mathbb{Q}_\ell]$, and by observing the local invariant at ℓ of $[D] \in \text{Br}(\mathbb{Q})$, we deduce that $2 \mid f$. On the other hand, if $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ does not split (that is, D remains a division algebra after tensoring with $\mathbb{Q}(\zeta_d)$), then by the definition of similarity we must have $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_d)'$, and so $2 \mid n_d$. Thus, $(C3) \Rightarrow (C7)$.

Next, we show that $(C5) \Rightarrow (C8)$. If $n_d \neq 1$, $(C8)$ always holds. So let us assume that $n_d = 1$. By Proposition 6.5 and Lemma 6.6, we may view F as an element of $\mathbb{Q}(\zeta_d)$. Since the characteristic polynomial of F has coefficients in \mathbb{Z} with constant

term a power of ℓ , we see that

$$(6.14) \quad F \in \mathbb{Z}[\zeta_d] \cap \mathbb{Z}[\zeta_d][\frac{1}{\ell}]^\times.$$

Moreover, since the action of F on $V_{\ell'}(B_d)$ is given by the scalar action of $\mathbb{Q}(\zeta_d) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$ on the rank one free $\mathbb{Q}(\zeta_d) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$ -module $V_{\ell'}(B_d)$, F must be an $\ell^{f_\lambda f_{\lambda/\ell}}$ -Weil number (when viewed as an element of $\mathbb{Q}(\zeta_d)$). Let $c \in G := \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ denote the restriction of complex conjugation to $\mathbb{Q}(\zeta_d)$. We must have $F^c F = \ell^{f_\lambda f_{\lambda/\ell}}$.

As $\ell \nmid d$ by (A4), the ideal $(\ell)\mathbb{Z}[\zeta_d]$ splits as a product of distinct prime ideals in $\mathbb{Z}[\zeta_d]$. Let $\lambda_1, \dots, \lambda_r$ be these prime ideals, where $r = \varphi(d)/f$. By (6.14), the prime ideal factorization of the principal ideal (F) must be

$$(F) = \lambda_1^{m_1} \lambda_2^{m_2} \dots \lambda_r^{m_r}.$$

Let $D_\ell \leq G$ be the decomposition group of ℓ (or equivalently, any of the λ_i). Under the isomorphism $G \cong (\mathbb{Z}/d\mathbb{Z})^\times$, c corresponds to $-1 \pmod{d}$. Further, D_ℓ corresponds to the subgroup $\langle \ell \pmod{d} \rangle$. Hence, the condition $c \in D_\ell$ is equivalent to (C2). So, if $c \in D_\ell$, we have (C2) \Rightarrow (C6) \Rightarrow (C7) \Rightarrow (C8).

In case $c \notin D_\ell$, then r is even, and $\lambda_i^c \neq \lambda_i$ for every $1 \leq i \leq r$. Relabel the ideals so that $\lambda_{2j-1}^c = \lambda_{2j}$. Now,

$$\begin{aligned} (\lambda_1 \lambda_2 \dots \lambda_r)^{f_\lambda f_{\lambda/\ell}} &= (\ell^{f_\lambda f_{\lambda/\ell}}) \\ &= (F^c \cdot F) = (\lambda_1 \lambda_2)^{m_1+m_2} \dots (\lambda_{r-1} \lambda_r)^{m_{r-1}+m_r}, \end{aligned}$$

and so

$$f_\lambda \cdot f_{\lambda/\ell} = m_1 + m_2 = \dots = m_{r-1} + m_r.$$

For the sake of contradiction, suppose (C8) does not hold; i.e., $f_\lambda f_{\lambda/\ell} = 1$. Then clearly $m_i = 0$ for exactly half of the indices i . But (under a suitable normalization) the $\{m_i\}$ represent the slopes of the Newton polygon of B_d . More specifically, the slopes are given by:

$$\underbrace{\frac{m_1}{f_\lambda f_{\lambda/\ell}}, \dots, \frac{m_1}{f_\lambda f_{\lambda/\ell}}}_{f \text{ times}}, \underbrace{\frac{m_2}{f_\lambda f_{\lambda/\ell}}, \dots, \frac{m_2}{f_\lambda f_{\lambda/\ell}}}_{f \text{ times}}, \dots, \underbrace{\frac{m_r}{f_\lambda f_{\lambda/\ell}}, \dots, \frac{m_r}{f_\lambda f_{\lambda/\ell}}}_{f \text{ times}},$$

But this implies the Newton polygon has $f \cdot \frac{r}{2}$ slopes of value 0, and (as $n_d = 1$), this implies $\gamma_d = g_d > 0$, which contradicts (C5). Thus, (C5) \Rightarrow (C8).

Finally, we show, assuming $n_d = 1$, that (C2) \Rightarrow (C3). Assuming (C2), we have $c \in D_\ell$, and $\lambda_i^c = \lambda_i$ for all i . So $(F^c) = (F)$. We consider the prime factorization:

$$\begin{aligned} (\lambda_1 \lambda_2 \dots \lambda_r)^{f_\lambda f_{\lambda/\ell}} &= (\ell^{f_\lambda f_{\lambda/\ell}}) \\ &= (F^c \cdot F) = (F)^2 = \lambda_1^{2m_1} \lambda_2^{2m_2} \dots \lambda_r^{2m_r}, \end{aligned}$$

which gives $f_\lambda f_{\lambda/\ell} = 2m_i$ for every i . Again we interpret this in terms of the Newton polygon of B_d , and see that every slope is $\frac{m_i}{f_\lambda f_{\lambda/\ell}} = \frac{1}{2}$. This is equivalent to the condition that B_d is supersingular, i.e., (C3). \square

7. UNCONDITIONAL RESULTS

In this section, we apply the results of §6 to obtain as many finiteness results as possible without the assumption of GRH.

7.1. Unconditional finiteness results over \mathbb{Q} . When $[A] \in \mathcal{A}(\mathbb{Q}, g, \ell)$, note that $e = e_{A_{\mathbb{Q}, \ell}}$ always. Already the finiteness of $\mathcal{A}(\mathbb{Q}, 1)$ has been established in [RT08]. The information coming from the special fiber allows us to settle the conjecture over \mathbb{Q} for $g \leq 3$.

Proposition 7.1. *The set $\mathcal{A}(\mathbb{Q}, 2)$ is finite.*

Proof. Suppose $\ell \gg 0$ and $[A] \in \mathcal{A}(\mathbb{Q}, 2, \ell)$. By Proposition 4.4, $m_{\mathbb{Q}} > 6$. But this is impossible under the condition $4 = \sum n_d \varphi(d)$. To see this, note that

$$\{d : \varphi(d) \leq 4\} = \{1, 2, 3, 4, 5, 6, 8, 10, 12\}.$$

Thus, the condition $4 \mid e$ (Lemma 3.5) implies one of n_{12} , n_8 , n_4 must be positive. The only solution with $n_{12} > 0$ is $4 = \varphi(12)$; in this case, $e = 12$ and $m_{\mathbb{Q}} \mid 6$. Likewise, $n_8 > 0$ only for the solution $4 = \varphi(8)$. In this case, $e = 8$ and $m_{\mathbb{Q}} \mid 4$. There are a handful of equations with $n_4 > 0$; each, however, has $e = 4$ or $e = 12$, and so $m_{\mathbb{Q}} \mid 6$. By contradiction, $\mathcal{A}(\mathbb{Q}, 2, \ell)$ must be empty. \square

Proposition 7.2. *The set $\mathcal{A}(\mathbb{Q}, 3)$ is finite.*

Proof. Suppose $\ell \gg 0$ and $[A] \in \mathcal{A}(\mathbb{Q}, 3, \ell)$. As in the case $g = 2$, the conditions $6 = \sum n_d \varphi(d)$ and $4 \mid e$ imply $m_{\mathbb{Q}} \leq 6$, with only four exceptions:

$$\begin{aligned} 6 &= \varphi(8) + \varphi(6) \\ 6 &= \varphi(8) + \varphi(3) \\ 6 &= \varphi(4) + \varphi(10) \\ 6 &= \varphi(4) + \varphi(5) \end{aligned}$$

So we may assume A has a decomposition corresponding to one of the above exceptions. For each exception, the only *possible* value for $m_{\mathbb{Q}}$ is $\frac{e}{2}$, as every other even divisor of $\frac{e}{2}$ is at most 6. However, in each case we observe a choice of d such that $n_d = 1$ and $d \mid \frac{e}{2}$. Let f denote the order of $\ell \pmod{d}$. We may be sure that $\gamma_d = 0$ (cf. the discussion of ℓ -rank in §3.3). Since $K = \mathbb{Q}$, we have $f_{\lambda/\ell} f_{\lambda} = f$. Hence, by Proposition 6.7, $n_d f \neq 1$, and so $f \neq 1$. This forces $d \nmid (\ell - 1)$, and so $d \nmid m_{\mathbb{Q}}$. Consequently, $m_{\mathbb{Q}} < \frac{e}{2}$, and by contradiction, $\mathcal{A}(\mathbb{Q}, 3, \ell) = \emptyset$. \square

Unconditional finiteness in the case $g = 4$ is not settled, but we have the following description of possible decompositions of the special fiber.

Proposition 7.3. *If $\ell \gg 0$ and $[A] \in \mathcal{A}(\mathbb{Q}, 4, \ell)$, then the decomposition of A corresponds to one of the following sums, and ℓ must satisfy congruence conditions as follows:*

Sum	Congruence
$2\varphi(3) + \varphi(8)$	$\ell \equiv 13 \pmod{24}$
$2\varphi(6) + \varphi(8)$	$\ell \equiv 13 \pmod{24}$
$\varphi(16)$	$\ell \equiv 9 \pmod{16}$
$\varphi(20)$	$\ell \equiv 11 \pmod{20}$
$\varphi(24)$	$\ell \equiv 13 \pmod{24}$

Proof. Take $\ell \gg 0$ and $[A] \in \mathcal{A}(\mathbb{Q}, 4, \ell)$. If the decomposition of A does not correspond to one of those given in the table, then by arguments similar to the previous cases, one may show that $m_{\mathbb{Q}} \leq 6$. However, the five cases above remain valid. For example, in case $n_3 = 2$ and $n_8 = 1$, we have $e = 24$, and the available results do not eliminate the possibility $m_{\mathbb{Q}} = 12$. We may conclude only that $\ell \equiv 1 \pmod{12}$ and $\ell \not\equiv 1 \pmod{8}$, i.e., $\ell \equiv 13 \pmod{24}$. The congruences in the remaining cases may be deduced similarly. \square

7.2. Finiteness of $\mathcal{A}(K, 1)$ when $n_K = 2$. In the authors' earlier work, it was shown that $\mathcal{A}(K, 1)$ must be finite when K/\mathbb{Q} is a quadratic extension, except possibly when K is imaginary with class number one [RT08, Thm. 4]. There, the proof uses the result of Momose [Mom95] (generalizing the previous work of Mazur [Maz78]) classifying K -rational points on modular curves. We give a different proof, which removes the exception for imaginary fields with class number one. The new proof relies on the theorem of Goldfeld from §2.

Proposition 7.4. *Suppose $n_K = 2$. Then the set $\mathcal{A}(K, 1)$ is finite.*

Proof. If $\mathcal{A}(K, 1)$ is infinite, then we may choose ℓ and $[A]$ so that $\ell > C_2(K)$, $\ell \nmid \Delta_K$, and $[A] \in \mathcal{A}(K, 1, \ell)$. The only solution to $2 = \sum n_d \varphi(d)$ for which $4 \mid e$ is $2 = \varphi(4)$. So in fact $e = 4$ and $m_{\mathbb{Q}} = 2$. By Corollary 2.4, there exists $p < \frac{\ell}{4}$, which is a square residue modulo ℓ . Moreover, $f_{\mathfrak{p}/p} = 1$ for any prime \mathfrak{p} of K above p . Consequently, $\chi(2)(\text{Frob}_{\mathfrak{p}}) = \chi(2)(\text{Frob}_p) = 1$. However, by Proposition 4.2, $\chi(2)(\text{Frob}_{\mathfrak{p}}) \neq 1$. By contradiction, $\mathcal{A}(K, 1)$ is finite. \square

Remark. Unfortunately, since Goldfeld's result is not effective, Proposition 7.4 is not effective, even for a particular choice of quadratic field K , and cannot be made uniform at present.

7.3. Additional finiteness results when $g = 1$. We present two more unconditional finiteness results. The first establishes finiteness for cubic fields in a uniform manner; that is, there exists a bound N such that $\ell > N$ implies $\mathcal{A}(K, 1, \ell) = \emptyset$ for any cubic field K . The second result is not uniform, but provides finiteness for $\mathcal{A}(K, 1)$ for any Galois extension K/\mathbb{Q} whose Galois group has exponent 3.

We begin with the result for cubic fields. We require an extension of the result of Proposition 4.2. Let K/\mathbb{Q} be a finite extension, and suppose $[A] \in \mathcal{A}(K, 1, \ell)$. Note that as (A2) holds for $\ell > C_7$, which depends only on g and n_K , we may use the results of §5 without invalidating uniformity.

Provided $\ell > 3$, for each prime $\lambda \mid \ell$ in K , we have a decomposition of $V_{\ell'}(A_{K_{\lambda}})^{\text{ss}}$ which yields

$$2 = 2g = \sum_{d|e_{A_{K_{\lambda}}}} n_d \varphi(d), \quad e_{A_{K_{\lambda}}} = \text{lcm}\{d : n_d > 0\}.$$

(Note that the collection $\{n_d\}$ depends on λ , even though this is suppressed in the notation.) Necessarily, $e_{A_{K_{\lambda}}} \in \{1, 2, 3, 4, 6\}$.

Proposition 7.5. *Conjecture 2 holds in case $(g, d) = (1, 3)$.*

Proof. In this case, we take $\ell > C_7(1, 3) > 3$ so that the above relations hold, and that further $4 \mid e := \gcd\{e_{A_{K_{\lambda}}} e_{\lambda/\ell} : \lambda \mid \ell\}$. Additionally, we have $m_{\mathbb{Q}} \mid (\frac{e}{2}, \ell - 1)$. As K is a cubic extension, we have $\sum_{\lambda \mid \ell} e_{\lambda/\ell} f_{\lambda/\ell} = n_K = 3$. If there exists a prime $\lambda \mid \ell$ for which $e_{\lambda/\ell} = 1$, then as $4 \mid e_{A_{K_{\lambda}}} e_{\lambda/\ell}$, we must have $e_{A_{K_{\lambda}}} = 4$, and

consequently $e = 4$. The only other possibility is that there is a unique prime $\lambda \mid \ell$, for which $e_{\lambda/\ell} = 3$. In this case, we have $e_{A_{K_\lambda}} = 4$, $e = 12$. Consequently, we may be sure that $m_{\mathbb{Q}} = 2$ or $m_{\mathbb{Q}} = 6$.

Choose $0 < \varepsilon < \frac{1}{12}$. By Proposition 2.1, there exists $p = O(\ell^{\frac{1}{4}+\varepsilon})$ such that $\chi(2)(\text{Frob}_p) = 1$. As $n_K = 3$, we may always choose $\mathfrak{p} \mid p$ in K such that $f_{\mathfrak{p}/p} \in \{1, 3\}$. Let $q = \#\kappa(\mathfrak{p})$. We have $q \leq p^3 = O(\ell^{\frac{3}{4}+3\varepsilon})$. There is an absolute constant C_{10} , independent of K , for which $\ell > C_{10}$ guarantees $q < \frac{\ell}{4}$. Below, we give a mild extension of Proposition 4.2, showing that $\chi(2)(\text{Frob}_{\mathfrak{p}}) \neq 1$. But this is a contradiction, since $\chi(2)(\text{Frob}_{\mathfrak{p}}) = \chi(2)(\text{Frob}_p)^{f_{\mathfrak{p}/p}} = 1$. \square

Proposition 7.6. *Suppose $n_K = 3$, $\ell > C_7(1, 3)$, and $[A] \in \mathcal{A}(K, 1, \ell)$. Let p be a rational prime, and $\mathfrak{p} \mid p$ a prime in K . If $f_{\mathfrak{p}/p}$ is odd and $q = \#\kappa(\mathfrak{p}) < \frac{\ell}{4}$, then $\chi(2)(\text{Frob}_{\mathfrak{p}}) \neq 1$.*

Proof. By Proposition 4.2, we already have $\chi(m_{\mathbb{Q}})(\text{Frob}_{\mathfrak{p}}) \neq 1$. If $m_{\mathbb{Q}} = 2$, we are done. Otherwise, we have $\chi(6)(\text{Frob}_{\mathfrak{p}}) \neq 1$. For the sake of contradiction, suppose that $\chi(2)(\text{Frob}_{\mathfrak{p}}) = 1$. Then $\chi(6)(\text{Frob}_{\mathfrak{p}})$ has exact order 3; so $\varepsilon_{r,r}(\text{Frob}_{\mathfrak{p}})$ must be exactly of order 3 for some $r \in \{1, 2\}$. Since the determinant of $\rho_{A,\ell}$ must be χ , we have $\chi^{i_1}\chi^{i_2} = \chi$; that is, $i_2 \equiv 1 - i_1 \pmod{\ell - 1}$. Hence,

$$\varepsilon_{1,1}\varepsilon_{2,2} = \chi^{2i_1-1}\chi^{2i_2-1} = 1.$$

Let $\omega = \varepsilon_{1,1}(\text{Frob}_{\mathfrak{p}}) \in \mathbb{F}_\ell^\times$. It is necessarily a primitive cube root of unity in \mathbb{F}_ℓ , and so $\varepsilon_{2,2}(\text{Frob}_{\mathfrak{p}}) = \omega^2$. Computing the trace of $\text{Frob}_{\mathfrak{p}}^2$, we have

$$\begin{aligned} a_{\mathfrak{p},2} &= \chi^{i_1}(\text{Frob}_{\mathfrak{p}}^2) + \chi^{i_2}(\text{Frob}_{\mathfrak{p}}^2) \\ &= (\varepsilon_{1,1}(\text{Frob}_{\mathfrak{p}}) + \varepsilon_{2,2}(\text{Frob}_{\mathfrak{p}})) \chi(\text{Frob}_{\mathfrak{p}}) \\ &\equiv -q \pmod{\ell}. \end{aligned}$$

As $|a_{\mathfrak{p},2}| \leq 2q$ by the Weil conjectures and $q < \frac{\ell}{4}$, we have $a_{\mathfrak{p},2} = -q$. Thus, the eigenvalues $\alpha_{\mathfrak{p},j}^2$ (in $\bar{\mathbb{Q}}$) for $\text{Frob}_{\mathfrak{p}}^2$ are roots of $T^2 + qT + q^2$, hence are $\{\zeta q, \zeta^2 q\}$, where ζ denotes a primitive cube root of unity in $\bar{\mathbb{Q}}$. Consequently, the eigenvalues for $\text{Frob}_{\mathfrak{p}}$ over $\bar{\mathbb{Q}}$ are contained in $\{\pm\zeta\sqrt{q}, \pm\zeta^2\sqrt{q}\}$, and each of these possible eigenvalues has a minimal polynomial of degree 4 over $\bar{\mathbb{Q}}$. But this is absurd; the eigenvalues should have a minimal polynomial of degree 2 over $\bar{\mathbb{Q}}$. By contradiction, $\chi(2)(\text{Frob}_{\mathfrak{p}}) \neq 1$. \square

We now turn to the result on Galois extensions of exponent 3.

Proposition 7.7. *Suppose K/\mathbb{Q} is a Galois extension and $\text{Gal}(K/\mathbb{Q})$ has exponent 3. Then the set $\mathcal{A}(K, 1)$ is finite.*

Proof. Take $\ell \gg 0$. Suppose $[A] \in \mathcal{A}(K, 1, \ell)$. By avoiding the primes dividing Δ_K , we know the decomposition $2g = \sum n_d \varphi(d)$ corresponds to $n_4 = 1$, $e = 4$, and $m_{\mathbb{Q}} = 2$.

Let $0 < \varepsilon < \frac{1}{12}$. From Proposition 2.1, we know there exists a prime $p = O(\ell^{\frac{1}{4}+\varepsilon})$ which is a square modulo ℓ ; hence, $\chi(2)(\text{Frob}_p) = 1$. Let \mathfrak{p} be a prime in K above p of norm q . Because $\text{Gal}(K/\mathbb{Q})$ is exponent 3, we must have $f_{\mathfrak{p}/p} \in \{1, 3\}$. In particular $f_{\mathfrak{p}/p}$ is odd, and $q \leq p^3 = O(\ell^{\frac{3}{4}+3\varepsilon}) < \frac{\ell}{4g}$ if we take ℓ sufficiently large. By Proposition 4.2, we also have $\chi(2)(\text{Frob}_{\mathfrak{p}}) \neq 1$. This is a contradiction, since $\text{Frob}_{\mathfrak{p}} = \text{Frob}_p^{f_{\mathfrak{p}/p}}$. By contradiction, we have that $\mathcal{A}(K, 1, \ell)$ is empty for all large ℓ , and so $\mathcal{A}(K, 1)$ is finite. \square

APPENDIX

In §2, we noted the existence of a constant C_6 , such that $\ell > C_6$ implies

$$(7.1) \quad \left(\frac{\ell}{4g}\right)^{\frac{1}{n}} > C_3 \cdot (C_4 + C_5 \log \ell)^2.$$

We now give a brief derivation for a choice of C_6 . The principal tool will be the Lambert W -function; this is a multivalued complex function defined as follows: for every $z \in \mathbb{C}$, $W(z)$ is a solution to the equation $W(z) \exp W(z) = z$. The basic properties of $W(z)$ that we will need are all thoroughly explained in [CGH⁺96].

If we restrict our consideration to real values, there are only two branches of W of interest, which we denote $W_0(x)$ and $W_{-1}(x)$. The real function W_0 is an increasing function defined on $[-e^{-1}, \infty)$, and the real function W_{-1} is a decreasing function defined on $[-e^{-1}, 0)$. We have $-1 = W_0(-e^{-1}) = W_{-1}(-e^{-1})$; there are no real solutions for $x < -e^{-1}$. (All of this may be observed by naïvely ‘inverting’ the real function $x(w) = we^w$.)

Lemma 1. *Suppose c and N are positive constants, and $c \geq (\frac{e}{N})^N$. Then the largest real solution to the equation $x^{\frac{1}{N}} = \log(cx)$ is given by*

$$x_0 = x_0(c, N) = \frac{1}{c} \exp\left(-NW_{-1}\left(-\frac{1}{N}c^{-\frac{1}{N}}\right)\right).$$

Proof. From $x^{\frac{1}{N}} = \log(cx)$, we have

$$\begin{aligned} -\frac{1}{N}c^{-\frac{1}{N}} \cdot (cx)^{\frac{1}{N}} &= -\frac{1}{N} \log(cx), \\ -\frac{1}{N}c^{-\frac{1}{N}} &= -\frac{1}{N} \log(cx) \cdot \exp\left(-\frac{1}{N} \log(cx)\right). \end{aligned}$$

The assumptions guarantee $-\frac{1}{N}c^{-\frac{1}{N}} \in [-e^{-1}, 0)$, so by the definition of W_j , we see $-\frac{1}{N} \log(cx) = W_j\left(-\frac{1}{N}c^{-\frac{1}{N}}\right)$ for $j \in \{-1, 0\}$. Solving for x , we find

$$x = \frac{1}{c} \exp\left(-NW_j\left(-\frac{1}{N}c^{-\frac{1}{N}}\right)\right).$$

That the larger solution corresponds to the index $j = -1$ follows from the fact that $W_{-1} \leq W_0 < 0$ on $[-e^{-1}, 0)$. \square

For the remainder, we write W for the specific branch W_{-1} . At any point $x \in (-e^{-1}, 0)$, differentiating $W(x)e^{W(x)} = x$ yields

$$W'(x) = \frac{e^{-W(x)}}{1 + W(x)} = \frac{1}{x} \cdot \frac{W(x)}{1 + W(x)}.$$

As W is a decreasing function and $y/(1+y)$ is increasing for all $y \neq -1$, we have for any $x \in (-\frac{1}{4}, 0)$:

$$\frac{W(x)}{1 + W(x)} < \frac{W(-\frac{1}{4})}{1 + W(-\frac{1}{4})} \approx 1.867 \dots < 2.$$

We define

$$L(x) = \begin{cases} W(-\frac{1}{4}) & x \in [-e^{-1}, -\frac{1}{4}) \\ 2 \log(-x) & x \in [-\frac{1}{4}, 0) \end{cases}.$$

Lemma 2. *For all $x \in [-e^{-1}, 0)$, $-1 \geq W(x) \geq L(x)$.*

Proof. As W is decreasing, the inequality is clear for $x \leq -\frac{1}{4}$. Now, set $f(x) = W(x) - L(x)$, and observe $f(-\frac{1}{4}) > 0$. For $x > -\frac{1}{4}$, we have

$$f'(x) = \frac{1}{x} \cdot \left(\frac{W(x)}{1 + W(x)} - 2 \right) > 0,$$

since $x < 0$ and $W(x)/(1 + W(x)) < 2$. So $W(x) \geq L(x)$, as claimed. \square

Lemma 3. Suppose $c \geq (\frac{4}{N})^N$. Then $x_0 \leq c \cdot N^{2N}$.

Proof. We have $-\frac{1}{N}c^{-\frac{1}{N}} > -\frac{1}{4}$, and so, combining the previous Lemmas,

$$x_0 \leq \frac{1}{c} \exp \left(-N \cdot 2 \log \left(\frac{1}{N}c^{-\frac{1}{N}} \right) \right) = c \cdot N^{2N}. \quad \square$$

Corollary 4. If a positive integer ℓ satisfies (7.1), then

$$\ell \leq 16g^2 C_3^{2n} C_5^{4n} (2n)^{4n} \exp \left(\frac{C_4}{C_5} \right).$$

Proof. We rewrite the inequality (7.1) as

$$x^{\frac{1}{N}} > \log(cx), \quad x = \frac{\ell}{4gC_3^n C_5^{2n}}, \quad N = 2n, \quad c = 4gC_3^n C_5^{2n} \exp \left(\frac{C_4}{C_5} \right).$$

We observe that $c \geq 4 \geq (\frac{4}{N})^N$. Thus, $x \leq x_0 \leq c \cdot N^{2N}$, and the claim follows immediately. \square

REFERENCES

- [AI88] G. Anderson and Y. Ihara. Pro- ℓ branched coverings of \mathbf{P}^1 and higher circular ℓ -units. *Ann. of Math.* (2), 128(2):271–293, 1988.
- [CGH⁺96] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W function. *Adv. Comput. Math.*, 5(4):329–359, 1996.
- [Coh77] Paul Moritz Cohn. *Algebra. Vol. 2.* John Wiley & Sons, London-New York-Sydney, 1977.
- [Ell71] P. D. T. A. Elliott. The least prime k -th-power residue. *J. London Math. Soc.* (2), 3:205–210, 1971.
- [GL06] Robert M. Guralnick and Martin Lorenz. Orders of finite groups of matrices. In *Groups, rings and algebras*, volume 420 of *Contemp. Math.*, pages 141–161. Amer. Math. Soc., Providence, RI, 2006.
- [HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L -functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc.* (3), 64(2):265–338, 1992.
- [Iha86] Y. Ihara. Profinite braid groups, Galois representations and complex multiplications. *Ann. of Math.* (2), 123(1):43–106, 1986.
- [Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.
- [Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
- [Min1887] Hermann Minkowski. Zur theorie der positiven quadratischen formen. *J. reine angew. Math.*, (101):196–202, 1887.
- [Mom95] F. Momose. Isogenies of prime degree over number fields. *Compositio Math.*, 97(3):329–348, 1995.
- [PR07] Matthew Papanikolas and Christopher Rasmussen. On the torsion of Jacobians of principal modular curves of level 3^n . *Arch. Math. (Basel)*, 88(1):19–28, 2007.
- [Ras04] C. Rasmussen. On the fields of 2-power torsion of certain elliptic curves. *Math. Res. Lett.*, 11(4):529–538, 2004.

- [RT08] C. Rasmussen and A. Tamagawa. A finiteness conjecture on abelian varieties with constrained prime power torsion. *Mathematical Research Letters*, 15(5–6):1223–1232, 2008.
- [Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [Ser79] Jean-Pierre Serre. Arithmetic groups. In *Homological group theory (Proc. Sympos., Durham, 1977)*, volume 36 of *London Math. Soc. Lecture Note Ser.*, pages 105–136. Cambridge Univ. Press, Cambridge, 1979.
- [SGA7I] *Groupes de monodromie en géométrie algébrique. I*. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.
- [Tam95] Akio Tamagawa. The Eisenstein quotient of the Jacobian variety of a Drinfel’d modular curve. *Publ. Res. Inst. Math. Sci.*, 31(2):203–246, 1995.
- [TO70] John Tate and Frans Oort. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)*, 3:1–21, 1970.

WESLEYAN UNIVERSITY, MIDDLETON, CONNECTICUT 06459, UNITED STATES
E-mail address: crasmussen@wesleyan.edu

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO 606-8502, JAPAN
E-mail address: tamagawa@kurims.kyoto-u.ac.jp